



02D03

520.38691X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): KAMINAGA, et al.  
Serial No.: 09/599,005  
Filed: June 22, 2000  
Title: INFORMATION PROCESSING DEVICE, CARD DEVICE  
AND INFORMATION PROCESSING SYSTEM

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

July 21, 2000

Sir:

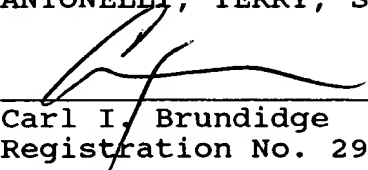
Under the provisions of 35 USC 119 and 37 CFR 1.55, the  
applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 11-178750  
Filed: June 24, 1999

A certified copy of said Japanese Patent Application is  
attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
\_\_\_\_\_  
Carl I. Brundidge  
Registration No. 29,621

CIB/ssr  
Attachment

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出 願 年 月 日  
Date of Application:

1999年 6月24日

出 願 番 号  
Application Number:

平成11年特許願第178750号

出 願 人  
Applicant (s):

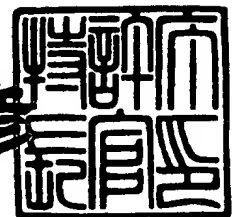
株式会社日立製作所  
株式会社日立超エル・エス・アイ・システムズ

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 6月16日

特 許 庁 長 官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3045650

【書類名】 特許願

【整理番号】 PNT990072

【提出日】 平成11年 6月24日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/14320

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内

【氏名】 神永 正博

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内

【氏名】 遠藤 隆

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内

【氏名】 大木 優

【発明者】

【住所又は居所】 東京都小平市上水本町5丁目22番1号 株式会社日立超エル・エス・アイ・システムズ内

【氏名】 塚元 卓

【発明者】

【住所又は居所】 東京都小平市上水本町5丁目22番1号 株式会社日立超エル・エス・アイ・システムズ内

【氏名】 渡瀬 弘

【発明者】

【住所又は居所】 東京都小平市上水本町五丁目20番1号 株式会社日立製作所半導体グループ内

【氏名】 寺内 千晶

【発明者】

【住所又は居所】 東京都小平市上水本町五丁目 2 0 番 1 号 株式会社日立  
製作所半導体グループ内

【氏名】 中田 邦彦

【発明者】

【住所又は居所】 東京都小平市上水本町五丁目 2 2 番 1 号 株式会社日立  
超エル・エス・アイ・システムズ内

【氏名】 長崎 信孝

【発明者】

【住所又は居所】 東京都小平市上水本町 5 丁目 2 2 番 1 号 株式会社日立  
超エル・エス・アイ・システムズ内

【氏名】 平 聡

【発明者】

【住所又は居所】 東京都小平市上水本町 5 丁目 2 2 番 1 号 株式会社日立  
超エル・エス・アイ・システムズ内

【氏名】 成吉 雄一郎

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日  
立製作所システム開発研究所内

【氏名】 福澤 寧子

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000233169

【氏名又は名称】 株式会社日立超エル・エス・アイ・システムズ

【代理人】

【識別番号】 100061893

【弁理士】



【氏名又は名称】 高橋 明夫

【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100086656

【弁理士】

【氏名又は名称】 田中 恭助

【電話番号】 03-3661-0071

【手数料の表示】

【予納台帳番号】 011626

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、カード部材および情報処理システム

【特許請求の範囲】

【請求項 1】 情報処理装置と、当該第 1 の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項 2】 第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第 1 もしくは第 2 の情報処理装置の少なくとも一方よりの信号を伝達する前記信号線での第 1 の電力の消費状態に対応して第 2 の電力の消費状態が定められ、且つ前記信号線での第 1 の電力の消費と前記第 2 の電力の消費とが互いに相反する期間に可能とされていることを特徴とする情報処理装置。

【請求項 3】 情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置の信号を伝達する前記信号線での第 1 の電力の消費状態に対応して第 2 の電力の消費状態が定められ、且つ前記信号線での第 1 の電力の消費と前記第 2 の電力の消費との和が所望値となされるごとく構成されたことを特徴とする情報処理装置。

【請求項 4】 情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置の信号を伝達する前記信号線での第 1 の電力の消費状態に対応して第 2 の電力の消費状態が定められ、且つ前記信号線での第 1 の電力の消費がなされる期間では、前記第 2 の電力の消費がなされず、前記信号線での第 1 の電力の消費がなされない期間では第 2 の電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項 5】 情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置のデジタル信号を伝達する前記信号線での信号値の反転に対応して電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項 6】 第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第 1 もしくは第 2 の情報処理装置の少なくとも一方よりのデジタル信号に基づく前記信号線での第 1 の電力の消費状態に対応して、前記信号線での転送信号の信号値の反転に対応して第 2 の電力の消費がなされる手段を有することを特徴とする情報処理装置。

【請求項 7】 情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能なことを特徴とする情報処理装置。

【請求項 8】 第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第 1 の情報処理装置あるいは第 2 の情報処理装置の少なくとも 1 者と前記信号線との間において、前記第 1 の情報処理装置あるいは第 2 の情報処理装置よりの信号を暗号化し、且つ前記信号線より転送されてくる信号を復号化することが可能なことを特徴とする情報処理装置。

【請求項 9】 第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第 1 の情報処理装置よりの信号を暗号化し、当該暗号化された第 1 の情報処理装置よりの信号を復号化して第 2 の情報処理装置に入力し、且つ前記第 2 の情報処理装置の出力を暗号化し、当該暗号化された第 2 の情報処理装置よりの信号を復号化して第 1 の情報処理装置に入力することが可能なことを特徴とする情報処理装置。

【請求項 10】 情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能なことを特徴とする情報処理装置。

【請求項 11】 情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報を復号化して、前記信号線を介して前記情報処理装置に入力が可能なことを特徴とする情報処理装置。

【請求項 12】 情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの出力される信号列が、その順序を異にして前記信号線を伝達され、且つ前記信号列の異にされた順序を復元が可能なことを特徴とする情報処理装置。

【請求項 13】 第 1 のデータ処理装置と、第 2 のデータ処理装置と、この両者を接続する信号線と、制御信号発生手段と、前記信号線で消費される第 1 の電力と、当該信号線での電力消費とは別の第 2 の電力を消費する手段とを少なくとも有し、前記第 1 あるいは第 2 のデータ処理装置は前記第 2 の電力を消費する手段に接続され、前記制御信号発生手段よりの制御信号によって当該信号線に搭載された信号をクリアしない制御方式で制御され、前記第 1 と第 2 のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第 1 の電力消費と前記第 2 の電力消費の和が所定値になるように、前記制御信号発生手段からの信号に応じて、前記第 1 あるいは第 2 のデータ処理装置から出力された信号と、当該信号の転送の直前に前記信号線に乗っている信号と、当該信号の転送の直前に充放電装置に入力された信号に対して、排他的論理和を求め、その出力信号を前記第 2 の電力を消費する手段への入力可能なことを特徴とする情報処理装置。

【請求項 14】 第 1 のデータ処理装置と、第 2 のデータ処理装置と、この両者を接続する信号線と、制御信号発生手段と、前記信号線で消費される第 1 の電力と、当該信号線での電力消費とは別の第 2 の電力を消費する手段とを少なくとも有し、前記第 1 および第 2 のデータ処理装置は各々前記第 2 の電力を消費する第 1 の手段および前記第 2 の電力を消費する第 2 の手段に接続され、前記制御信号発生手段よりの制御信号によって当該信号線に搭載された信号をクリアしない制御方式で制御され、前記第 1 と第 2 のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第 1 の電力消費と前記第 2 の電力消費の和が所定値になるように、前記制御信号発生手段からの信号に応じて、前記第 1 あるいは第 2 のデータ処理装置から出力された信号と、当該信号の転送の直前に前記信号線に乗っている信号と、当該信号の転送の直前に充放電装置に入力された信号に対して、排他的論理和を求め、その出力信号を前記第 2 の電力を消費する手段への入力可能なことを特徴とする情報処理装置。

【請求項 1 5】 前記第 2 の電力を消費する第 2 の手段はダミー信号線を有することを特徴とする請求項 1、2 のいずれかに記載の情報処理装置。

【請求項 1 6】 前記第 2 の電力を消費する第 2 の手段はダミー信号線を有することを特徴とする請求項 1、2 のいずれかに記載の情報処理装置。

【請求項 1 7】 第 1 のデータ処理装置と、第 2 のデータ処理装置と、この両者を接続する信号線と、プリチャージ信号の制御手段と、前記信号線で消費される第 1 の電力と、当該信号線での電力消費とは別の第 2 の電力を消費する手段とを少なくとも有し、前記第 1 あるいは第 2 のデータ処理装置は前記第 2 の電力を消費する手段に接続され、且つ前記第 2 あるいは第 1 のデータ処理装置は前記プリチャージ信号の制御手段に接続され、前記第 1 と第 2 のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第 1 の電力消費と前記第 2 の電力消費の和が所定値となされるごとく構成されたことを特徴とする情報処理装置。

【請求項 1 8】 第 1 のデータ処理装置と、第 2 のデータ処理装置と、これらを接続する信号線と前記信号線をプリチャージするためのプリチャージ信号線制御装置を少なくとも有し、前記第 1 のデータ処理装置は、前記プリチャージ信号線制御装置に接続され、さらに相補的プリチャージバス制御装置にも接続され、前記プリチャージバス制御装置は、前記信号線に接続され、前記相補的プリチャージバス制御装置は前記信号線での第 1 の電力消費とは別の第 2 の電力を消費する手段に接続され、前記データ信号線での第 1 の消費電力と前記第 2 の消費電力の和が所定値になるように、前記信号線のプリチャージ直後にバスに流すデータをビット反転して第 2 の電力を消費する手段に入力されることを有することを特徴とする情報処理装置。

【請求項 1 9】 前記第 2 の電力を消費する第 2 の手段はプリチャージダミー信号線を有することを特徴とする請求項 1 7 または 1 8 のいずれかに記載の情報処理装置。

【請求項 2 0】 第 1 のデータ処理装置と、第 2 のデータ処理装置と、これらをつなぐ信号線と、前記信号線をプリチャージするプリチャージ信号線制御手段とを少なくとも有し、前記信号線は、当該信号線の途中に反転装置を少なくとも有

し、当該反転装置を挟んで、正論理と負論理との信号線から構成されることを特徴とする情報処理装置。

【請求項 21】 信号の暗号化に用いる鍵情報を自動的に設定することが可能なことを特徴とする請求項 7 に記載の情報処理装置。

【請求項 22】 信号の暗号化の鍵情報の一部として、情報処理装置の有する記憶情報の番地情報を用いて暗号化あるいは復号化がなされる事を特徴とする請求項 7 に記載の情報処理装置。

【請求項 23】 信号の暗号化の鍵情報を設定あるいは変更する手段を有する暗号化あるいは復号化がなされる事を特徴とする請求項 7 に記載の情報処理装置。

【請求項 24】 信号の暗号化に用いた鍵情報及び復号化に必要な暗号情報を記憶する領域を有するデータ処理装置と、当該データ処理装置内に記憶された暗号情報に基づいて復号化がなされる事を特徴とする請求項 7 に記載の情報処理装置。

【請求項 25】 信号の暗号化あるいは復号化が、記憶装置を複数の領域に分割し、領域ごとに暗号化の有無を指定するための暗号化領域指定手段を有し、暗号化するか否かを記憶装置の領域に応じて指定可能な事を特徴とする請求項 7 に記載の情報処理装置。

【請求項 26】 信号の暗号化あるいは復号化が、特定のデータパターンに対しては暗号化を行わない事を特徴とする請求項 7 に記載の情報処理装置。

【請求項 27】 信号の暗号化に用いる鍵情報を自動的に設定が可能な事を特徴とする請求項 8 に記載の情報処理装置。

【請求項 28】 信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いて暗号化あるいは復号化をなす事を特徴とする請求項 8 に記載の情報処理装置。

【請求項 29】 信号の暗号化に用いる鍵情報を定期的に自動再設定が可能な事を特徴とする請求項 8 に記載の情報処理装置。

【請求項 30】 信号の暗号化あるいは復号化に対しての暗号化の鍵情報を設定あるいは変更が可能なことを特徴とする請求項 8 に記載の情報処理装置。

【請求項 3 1】 データ処理装置と情報記憶装置と、これらを結ぶ信号線を少なくとも有し、前記データ処理装置と前記信号線の間で暗号化が可能であり、前記信号線と前記情報記憶装置との間で複号化が可能なることを特徴とする情報処理装置。

【請求項 3 2】 信号の暗号化に用いる鍵情報を自動的に設定が可能なることを特徴とする請求項 3 1 に記載の情報処理装置。

【請求項 3 3】 暗号化に用いる鍵情報を定期的に自動再設定が可能なることを特徴とする請求項 3 1 に記載の情報処理装置。

【請求項 3 4】 信号の暗号化あるいは複号化に対しての暗号化の鍵情報を設定あるいは変更が可能なることを特徴とする請求項 3 1 に記載の情報処理装置。

【請求項 3 5】 複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別して、記録あるいは読み出しが可能であり、情報を格納する際に情報を暗号化し、情報を読み出す際の複号化が可能なることを特徴とする情報記憶装置。

【請求項 3 6】 信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いる事を特徴とした請求項 3 5 に記載の情報記憶装置。

【請求項 3 7】 信号の暗号化鍵を自動的に初期化することが可能なることを特徴とする請求項 3 5 に記載の情報記憶装置。

【請求項 3 8】 信号の暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする、暗号化領域判定装置を有する事を特徴とする請求項 3 5 に記載の情報記憶装置。

【請求項 3 9】 信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いる事を特徴とする請求項 9 に記載の情報記憶装置。

【請求項 4 0】 信号の暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする事を特徴とする請求項 9 に記載の情報記憶装置。

【請求項 4 1】 記憶装置と、記憶装置を含むデータ処理装置と、それらを結ぶ信号線と、記憶装置と記憶装置を含むデータ処理装置との間の情報転送を制御する情報転送制御装置とを少なくとも有し、前記情報転送制御装置が、転送元の情報が格納された番地を記憶するためのアドレスレジスタと、転送先の番地を記憶するためのアドレスレジスタと、転送する情報の数をカウントするための数値を格納するカウンタと、カウンタの値をデクリメントするための演算回路と、記憶装置間で転送するデータを一時的に保存するデータバッファと、アドレスレジスタの値を更新するための演算回路と、転送アドレスの転送順番をランダム化する回路を有することを特徴とする情報処理装置。

【請求項 4 2】 情報処理装置と、当該第 1 の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とするカード部材。

【請求項 4 3】 端末機と、前記端末機に接続可能なカード部材とを少なくとも有し、前記カード部材は、情報処理装置と、当該第 1 の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理システム。

#### 【発明の詳細な説明】

【0001】

#### 【発明の属する技術分野】

本願発明は、高いセキュリティを持つ情報処理装置および情報記憶装置に関するものである。更には、本願発明は、カード部材および情報処理システムに関するものである。当該カード部材としては、特に IC カード（スマートカード）に代表される、1 チップの CPU（Central Processing Unit）を情報処理装置として内蔵するものをあげることが出来る。

【0002】

#### 【従来の技術】

IC カードに代表される高いセキュリティを持ったマイクロコンピュータチッ



ブでは、勝手に書き換えられない情報の保持や秘密情報である暗号鍵を使って秘匿すべきデータの暗号化や暗号文の復号化を行うことがある。

### 【0003】

マイクロコンピュータの基本構成は、図1に示すように、中央演算装置8001、記憶装置8002、そして各部の情報のやりとりを行うための道である信号線8003を有している。中央処理装置8001は、論理演算や算術演算などを行う装置であり、記憶装置8002は、プログラムやデータを格納する装置である。記憶装置8002は、例えばROM (Read Only Memory) やRAM (Random Access Memory)、EEPROM (Electrical Erasable Programmable Read Only Memory)、FRAM (Ferromagnetic Random Access Memory) などを用いて構成される。ROMは、変更できないメモリであり、主にプログラムを格納するメモリである。RAMは自由に書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消去される。従ってデバイスに電源の供給が中断されると、RAMの内容は、保持できなくなる。EEPROM、FRAMは、電源の供給が中断されてもその内容を保持することができるメモリである。

### 【0004】

例えば接触型ICカードに供されるコンピュータの本体の例を、図2に示す。図2にはこの半導体装置のチップ51の端子配置のみを示している。当該コンピュータの本体は、カードの中央の横に配置されたCOTと呼ばれるチップである。図2には端子配置の例が示されている。即ち、ICカードは、Vcc（供給電源）、GND（グランド）、RST（リセット）、I/O（入出力）、およびCLK（クロック）の端子を持つ。前記チップはこれらの信号を外部から、即ち、例えば端末機から、供給されることによって稼動する。尚、前記端末機自体は基本的に通例のカード・システムのものを用いて十分である。この場合、消費電力はVccとGNDとの信号を観察することによって測定することができる。この消費電力の測定については、John Wiley & sons社、W. Rankl W. Effing著1997年「Smart Card Handbook

」の 8.5.1.1 Passive protective mechanisms (263 ページ) に記載されている。

【0005】

【発明が解決しようとする課題】

本願発明の課題は、高いセキュリティを持つ情報処理装置を提供せんとするものである。当該情報処理装置としてはコンピュータシステム、わけてもマイクロコンピュータシステムを代表例としてあげることが出来る。

【0006】

更には、本願発明は、高いセキュリティを持つ、ICカード（スマートカード）に代表されるカード部材、およびカード・システムを提供するものである。

【0007】

本願発明のより技術的な課題を示せば、それは、マイクロコンピュータチップでのデータ処理と消費電力との関連性を減少させることである。特にICカードは、重要な情報を格納したり、カードの中で暗号処理を行うために用いられている。それは、プログラムや重要な情報がICカード用チップの中に密閉されているためである。ICカードでの暗号の解読は、暗号に対するアルゴリズムの解読の困難さと同程度と考えられていた。しかし、ICカードが暗号処理を行っている際の消費電力を観測し、この消費電力の状態を解析することにより、暗号処理の内容や暗号鍵が推定される可能性が示唆されている。この消費電力を観測する方法は、暗号に対するアルゴリズムの直接的な解読する方法よりも容易であると目されている。

【0008】

従って、消費電力とチップの処理との関連性が薄れれば、観測した消費電力の波形からICカードチップ内での処理や暗号鍵の推測が困難になる。本願発明の着眼点は、マイクロコンピュータの消費電力と処理されるデータとの関連を減少させることである。その手段の主なものは、消費電力の差を生み出す原因の一つである信号線（例えば、バスラインや、RAM内のビット線、ワード線等）の充放電を均一にするか、又は、元のデータと異なるものにすることによるものである。

【0009】

以下にまず、本願発明の背景となる消費電力の観測による、処理信の解読の可能性について説明する。このことが理解されれば、本願発明の趣旨が容易に理解されよう。

【0010】

上述の消費電力の測定の骨子は次の通りである。ICカード用チップの有するCMOS (Complementary Metal-Oxide-Semiconductor) のゲート回路は、出力状態が1から0あるいは0から1に変わった時に電力を消費する。特に信号線は大きな配線容量を持つため、当該ゲート回路は、バスのデータ値が1から0あるいは0から1に変わると、その充放電のために大きな電力を消費する。そのため、こうした消費電力を観測すれば、ICカード用チップの中での情報処理の内容が解読される可能性がある。

【0011】

図3は、ICカード用チップの1サイクルでの消費電力の波形を示したものである。処理している諸データの値に依存して、消費電力の諸波形が1101や1102のように異なる。このような複数の消費電力に対する波形の差は、信号線を通るデータや中央演算装置で処理しているデータ等に依存して生じる。

【0012】

現在、ICカード用チップの信号線の制御方式には、大別して二つの種類がある。一つはスタティック信号線制御方式であり、もう一つがプリチャージ信号線制御方式である。

【0013】

スタティック信号線制御方式は、バスに乗っているデータのクリアは行わないものである。一方、プリチャージ信号線制御方式は、一回の処理が終わる毎にデータをクリアするために、信号線のデータを全て1または0にしてから次のデータを乗せる制御方式である。尚、プリチャージを信号値の1か0のどちらにするかは、論理回路が順論理か、逆論理かで異なる。しかし、その動作の本質は変わらない。

【0014】

上述の基本動作の説明から明らかなように、この制御方式の違いにより、消費電力の波形が異なる。消費電力波形の違いから、どちらの制御方式を用いているかを判断する事ができる。

【0015】

信号線の制御方式がわかれば、暗号鍵は決まっているため、処理するデータを変更して、消費電力を観測することにより、暗号鍵のビット値の影響が観測できる可能性が生ずる。また、これらの消費電力の波形を分析することにより、暗号鍵を推定できる可能性が生ずる。

【0016】

【課題を解決するための手段】

本願発明の基本となる考え方をまず説明し、次いで、本願に開示される主な発明の諸形態を列挙する。本願発明の基本となる考え方は大きくは次の4つの方法に大別される。

【0017】

<1. 信号線の電力の消費の均一化>

第1の方法は、例えば情報処理装置における、例えばメモリの駆動方式やデータ内容に基づく消費電力の差を減少させる方法である。具体的には、この方法は、マイクロコンピュータ内部の信号線での電力の消費の他にも、例えば簡単には、前記信号線での電力消費に対応して、これとは別に充放電装置にて電力の消費を行うことによって、伝達される各信号列毎の消費電力の差を減少させるものである。

【0018】

<2. 信号線内のデータの暗号化>

第2の方法は、例えば情報処理装置において、信号線にのせるデータを暗号化し、当該信号線での電力消費を攪乱する方法である。即ち、この方法は、マイクロコンピュータ内部の信号線にデータを乗せる際に、データの暗号化を行い、データを受信する装置に入力する際にこのデータの復号化を行うものである。こうして、前記信号線での電力消費を攪乱することが出来る。

【0019】

## &lt;3. 記憶情報の暗号化&gt;

第3の方法は、例えば情報処理装置において、暗号化したデータを記憶部に格納する方法である。即ち、この方法は、例えばマイクロコンピュータの記憶装置に暗号化したデータを格納し、このデータの演算等を行う際に復号化して利用することにより、信号線での電力消費を攪乱するものである。

【0020】

## &lt;4. データ転送順序の交換&gt;

第4の方法は、例えば情報処理装置において、データ転送順序を変更する方法である。即ち、マイクロコンピュータの記憶装置に格納されているデータを信号線に載せて転送する際に、転送の順序を入れ替えることにより、信号線での電力消費を攪乱するものである。

【0021】

尚、必要に応じて、上記4つの発明の形態を組み合わせ、併用することが出来る。また、このような諸形態の併用によって、より有効に半導体装置の高セキュリティを確保することが出来る。この併用の諸例を例示すれば次のごとき方法である。

【0022】

それらは、(1) 信号線の電力の消費を均一化しつつ信号線内データの暗号化する方法、(2) 信号線の電力の消費を均一化しつつ記憶情報の暗号化を図る方法、(3) 電力の消費の均一化を図りつつデータ転送順序の交換する方法、(4) 信号線内データの暗号化しつつ記憶情報の暗号化を図る方法、(5) 信号線内データの暗号化しつつデータ転送順序の交換する方法、(6) 記憶情報の暗号化を図りつつデータ転送順序の交換する方法である。

【0023】

更に、2つ以上の方法を併用することも可能である。即ち、それらは(7) 信号線内データの暗号化しつつ信号線の電力の消費の均一化を図り、且つ記憶情報の暗号化を図る方法、(8) 信号線内データの暗号化しつつ信号線の電力の消費の均一化を図り、且つデータ転送順序の交換する方法、(9) 信号線内データの

暗号化しつつ記憶情報の暗号化を図り且つデータ転送順序の交換する方法、(10) 記憶情報の暗号化を図りつつデータ転送順序の交換し且つ信号線の電力の消費の均一化する方法である。更には、それは(11) 信号線の電力の消費の均一化、信号線内データの暗号化、記憶情報の暗号化、およびデータ転送順序の交換する方法である。

【0024】

以下、前記の4つの基本形態を柱として、それぞれの諸形態について詳細に説明する。

【0025】

(1) 信号線の電力の消費の均一化

本願の発明思想の第1は、前述の通り、例えば、メモリの駆動方式やデータ内容に基づく消費電力の差を減少させる方法である。

【0026】

この方法は、先に例示したマイクロコンピュータ内部の信号線での電力の消費の他にも、前記信号線でのデジタル・データの転送に伴う電力消費に対応する電力の消費を行なわせる手段、例えば簡単には、電荷の充放電する手段、装置を設けるものである。この充放電装置によって、前記信号線でのデジタル・データの転送に伴う電力消費に対応する電力を消費させ、上記伝達信号列によらずその消費電力の差を減少させるものである。即ち、当該マイクロコンピュータにおける信号線で消費される電力と、充放電装置において消費される電力の和を同一にするのである。各記憶装置の信号線に対する両消費電力の和が常に同一であれば、仮にデバイスの消費電力のデータが取り出せても、内部情報を知る事は非常に困難となる。

【0027】

尚、以下、電荷の充放電する手段、装置を単に充放電装置と称する。以下に説明するように、当該充放電装置として、例えばダミーデータ線を用いて構成することも出来る。

【0028】

本願発明に係わる一例では、上述の考え方にに基づき、マイクロコンピュータ内

部の2つのデータ処理装置を接続している信号線を介してデータの転送を行う際、このデータのデジタル信号に応じて、ビットを反転して充放電装置に入力し、当該信号線で消費される電力と、当該充放電装置で消費される電力の両者を同一にする。制御信号発生装置が発生する信号に応じて、定常消費電流発生装置を作動させることにより、当該信号線に乗せるデータを、充放電装置での消費電力と当該信号線で消費される電力が常に一定になるように、マイクロコンピュータチップの消費電力と処理しているデータの関連を減少させる。

## 【0029】

尚、前記2つのデータ処理装置は、具体的には、例えば、ROM、PROM、EPROM、EEPROM、RAM、FRAM等を有して構成されている。

## 【0030】

以下、信号線の制御方式の相違への対応を含めて本形態を説明する。即ち、入力されるビットデータは、信号線の制御方式によって異なる。

## 【0031】

いわゆる、CMOS回路では、ビット反転、すなわち、データが0から1または、1から0に変化する時、特に電力が消費される。このように、信号線では、ビット反転が起きるときに消費電力が大きくなる。従って、本願発明では、当該記憶装置に設けた充放電装置によって、前記ビット反転の回数に応じて充放電装置でも同様の電力消費を行うようにする。こうして、信号線で消費される電力と、充放電装置で消費される電力の両者の和が一定になり、信号線を通るデータとマイクロコンピュータチップの消費電力との関連性を緩和することができる。

## 【0032】

信号線におけるビット反転個数は、信号線の制御方式によってことなる。信号線の制御方式は、前述の通り、スタティック信号線制御方式とプリチャージ信号線制御方式とがある。その各々について説明する。

## 【0033】

まず、スタティック信号線制御方式の場合を考える。この場合、データはクリアされず、前のデータが信号線に残っている。実際の装置では、信号線は実質的に、コンデンサと同じ機能を持っている。従って、ここで前述の「残っている」

というのは、物理的には、電荷が残っているという意味である。従って、前に信号線に乗っていたデータの値を記憶しておけば、次に乗るデータに応じて、消費電力がどのように変わるかがわかる。

## 【0034】

この消費電力と充放電装置で消費される電力を同一にするためには、信号線で電力消費が行われるときには充放電装置に入力するデータは変化させず、信号線で電力消費が行われないときには、充放電装置に入力するデータを変化させ、両者の消費電力の合計が、常に一定になるようにする。この場合、消費電力は、内部処理のうち信号線を介さないものの消費電力を除いて、単一の信号線において常にビット反転が起こっている状態と同一になり、内部処理データと無関係となるため、内部処理データと消費電力の関連性を減少させることができる。

## 【0035】

一方、プリチャージ信号線制御方式においては、データの転送毎にデータが毎回クリアされる。従って、信号線での消費電力は、信号線に直前に乗っていたデータによらず、次に乗るデータを二進法表示したときに現れる1の個数に比例する。尚、逆論理なら信号線での消費電力は0の個数に比例する。

## 【0036】

従って、プリチャージ信号線制御方式の場合に、この消費電力と充放電装置で消費される電力を同一にするためには、データを信号線に乗せると同時に、このデータのビット反転値分を充放電装置に流す事である。こうして、信号線で消費される電力と、充放電装置で消費される電力の両者の消費電力の合計が、常に一定になるようにする。この場合も、マイクロコンピュータの消費電力は、内部処理のうち信号線を介さないものの消費電力を除いて、単一の信号線において常にビット反転が起こっている状態と同一になり、内部処理データと無関係となるため、内部処理データと消費電力の関連性を減少させることができる。

## 【0037】

多くのマイクロコンピュータチップの内部では、スタティック信号線制御方式と、プリチャージ信号線制御方式とが混在している。従って、マイクロコンピュータチップ全体の消費電力変化と処理データとの関連性を減少させるには、前述



の両方法を用いた情報処理装置を合わせて用いる必要がある。

【0038】

(2) 信号線に乗せるデータの暗号化

次に、信号線に乗せるデータを暗号化する方法について説明する。この方法によれば、信号線での消費電力は、実際のデータに基づく消費電力とは別のものになっている。従って、仮に、半導体装置より消費電力のデータが取り出せても、半導体装置の内部情報を知る事は困難となる。

【0039】

本発明の形態では、マイクロコンピュータ内部の2つのデータ処理装置（ROM、PROM、EPROM、EEPROM、RAM、FRAM等を有して構成されている）を接続している信号線を介してデータの転送を行う際、データを転送する側は定められた暗号化方式によって暗号化を行う暗号化装置によって暗号化したデータを転送する。一方、データを受信する装置は、この暗号化されたデータを復号化する復号化装置によって当該暗号化データを復号して処理を行う。このような処理によれば、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法による効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待することができる。

【0040】

(3) 記憶情報の暗号化

第3は、記憶装置に記憶させるデータを暗号化して格納する方法である。この方法は、例えば、読み出し専用のメモリであるROMにデータを書き込む際に定められた暗号化方式によってデータを暗号化してから格納する。このデータをデータ処理装置等で利用する際には、この暗号化されたデータを定められた方式によって復号化する復号化装置によって復号してからデータ処理装置に入力する。この方法では、信号線に乗る転送データは、暗号化されたデータとなり、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法による効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待する

ことができる。

【0041】

(4) データ転送順序の交換

第4は、信号線に乗せるデータの転送順序を元とは異なるものにする方法である。この方法は、例えば、転送するデータが、毎クロックおきに、A、B、C、D、Eの順序で転送されるところを、E、A、B、D、Cの順序で転送する。このデータの転送順序は勿論一例である。この方法により、信号線の充放電のパターンは、本来の順序通りに行われたい。従って、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法の効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待することができる。

【0042】

以下に本願発明の主な諸形態を列举する。

【0043】

本願発明の第1の形態は、情報処理装置と、当該第1の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理装置である。

【0044】

第2の形態は、第1の情報処理装置と、第2の情報処理装置と、その両者を結ぶ信号線とを有し、前記第1もしくは第2の情報処理装置の少なくとも一方よりの信号を伝達する前記信号線での第1の電力の消費状態に対応して第2の電力の消費状態が定められ、且つ前記信号線での第1の電力の消費と前記第2の電力の消費とが互いに相反する期間に可能とされていることを特徴とする情報処理装置である。

【0045】

第3の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置の信号を伝達する前記信号線での第1の電力の消費状態に対応して第2の電力の消費状態が定められ、且つ前記信号線での第1の電力の消

費と前記第 2 の電力の消費との和が所望値となされるごとく構成されたことを特徴とする情報処理装置である。

【0 0 4 6】

第 4 の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置の信号を伝達する前記信号線での第 1 の電力の消費状態に対応して第 2 の電力の消費状態が定められ、且つ前記信号線での第 1 の電力の消費がなされる期間では、前記第 2 の電力の消費がなされず、前記信号線での第 1 の電力の消費がなされない期間では第 2 の電力の消費が可能とされていることを特徴とする情報処理装置である。

【0 0 4 7】

第 5 の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置のデジタル信号を伝達する前記信号線での信号値の反転に対応して電力の消費が可能とされていることを特徴とする情報処理装置である。

【0 0 4 8】

第 6 の形態は、第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線と、前記第 1 もしくは第 2 の情報処理装置の少なくとも一方よりのデジタル信号に基づく前記信号線での第 1 の電力の消費状態に対応して、前記信号線での転送信号の信号値の反転に対応して第 2 の電力の消費がなされる手段を有することを特徴とする情報処理装置である。

【0 0 4 9】

第 7 の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能なことを特徴とする情報処理装置である。

【0 0 5 0】

第 8 の形態は、第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを有し、前記第 1 の情報処理装置あるいは第 2 の情報処理装置の少なくとも 1 者と前記信号線との間において、前記第 1 の情報処理装置あるいは第 2

の情報処理装置よりの信号を暗号化し、且つ前記信号線より転送されてくる信号を復号化することが可能なことを特徴とする情報処理装置である。

【 0 0 5 1 】

第 9 の形態は、第 1 の情報処理装置と、第 2 の情報処理装置と、その両者を結ぶ信号線とを有し、前記第 1 の情報処理装置よりの信号を暗号化し、当該暗号化された第 1 の情報処理装置よりの信号を復号化して第 2 の情報処理装置に入力し、且つ前記第 2 の情報処理装置の出力を暗号化し、当該暗号化された第 2 の情報処理装置よりの信号を復号化して第 1 の情報処理装置に入力することが可能なことを特徴とする情報処理装置である。

【 0 0 5 2 】

第 1 0 の形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能なことを特徴とする情報処理装置である。

【 0 0 5 3 】

第 1 1 の形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報を復号化して、前記信号線を介して前記情報処理装置に入力が可能なことを特徴とする情報処理装置である。

【 0 0 5 4 】

第 1 2 の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置よりの出力される信号列が、その順序を異にして前記信号線を伝達され、且つ前記信号列の異にされた順序を復元が可能なことを特徴とする情報処理装置である。

【 0 0 5 5 】

第 1 3 の形態は、情報処理装置と、当該第 1 の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていること

を特徴とするカード部材である。

【0056】

尚、本願は、それらの列挙は避けるが、ここに掲げた例以外に、前記の諸情報処理装置あるいは前記の諸情報記憶装置を有する諸カード部材を提供出来るものである。更には、本願は、後述する情報処理装置あるいは前記の諸情報記憶装置を有する諸カード部材を提供出来るものである。

【0057】

第14の形態は、端末機と、前記端末機に接続可能なカード部材とを少なくとも有し、前記カード部材は、情報処理装置と、当該第1の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とするカード・システムである。

【0058】

尚、本願は、その列挙は避けるが、この掲げた例以外に、前記情報処理装置あるいは前記情報記憶装置を有する諸カード・システムを提供出来るものである。更には、本願は、後述する情報処理装置あるいは前記の諸情報記憶装置を有する諸カード・システムを提供出来るものである。

【0059】

加えて、本願発明の更なる諸形態を列挙する。これらによって、本願発明の諸形態をより具体的に理解されるであろう。

【0060】

第15の形態は、二つのデータ処理装置A、Bとこれらを接続する信号線（制御信号によってバスラインのデータをクリアしない制御方式で制御される信号線：スタティック信号線）と、制御信号発生装置を有するマイクロコンピュータにおいて、該データ処理装置A、B間において該信号線を介して情報の転送を行う際、該信号線で消費される電力と、充放電装置で消費される電力の和が一定になるように、制御信号発生装置からの信号に応じて、データ処理装置Aから出力されたデータ（DATA）と、直前に該信号線に乗っているデータ（PBD）と、直前に充放電装置に入力されたデータ（CDD）に対して、以下の表1にしたが

って、充放電装置への入力を行い、信号線には、データ処理装置Aから出力されたデータ（DATA）を入力する為に該データ処理装置Aに接続された電力発生装置Cを有することを特徴とする情報処理装置である。

【0061】

【表1】

PBD	DATA	CDD	本願の充放電装置 への出力
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

表1

【0062】

尚、ここで、理解を容易とする為、本願明細書において、「電力発生装置」との用語を用いるが、これは、前述したように、信号線での電力の消費の他にも、前記信号線でのデータの転送に伴う電力消費に対応する電力の消費を行なわせる手段である。即ち、上記用語における「電力発生」とは信号線の電力の消費を均一化し、伝送する信号列によらず、基本的に同じ電力の消費を行うとの意味である。この装置が一般的に「電力を発生する」意でないことを注記して置く。

【0063】

第16の形態は、二つのデータ処理装置A、Bとこれらを接続する信号線（制御信号によってバスラインのデータをクリアしない制御方式で制御される信号線

：スタティック信号線）と、制御信号発生装置を有するマイクロコンピュータにおいて、該データ処理装置 A、B 間において該信号線を介して情報の転送を行う際、該信号線で消費される電力と、充放電装置で消費される電力の和が一定になるように、制御信号発生装置からの信号に応じて、データ処理装置 A から出力されたデータ（DATA）と、直前に該信号線に乗っているデータ（PBD）と、直前に充放電装置に入力されたデータ（CDD）に対して、上記の表 1 にしたがって、充放電装置への入力を行い、信号線には、データ処理装置 A から出力されたデータ（DATA）を入力する為に該データ処理装置 A、B それぞれに接続された電力発生装置 C、D（C と D が同一である場合を含む）を有することを特徴とする情報処理装置である。

## 【0064】

第 17 の形態は、第 1 のデータ処理装置と、第 2 のデータ処理装置と、この両者を接続する信号線と、プリチャージ信号の制御手段と、前記信号線で消費される第 1 の電力と、当該信号線での電力消費とは別の第 2 の電力を消費する手段とを少なくとも有し、前記第 1 あるいは第 2 のデータ処理装置は前記第 2 の電力を消費する手段に接続され、且つ前記第 2 あるいは第 1 のデータ処理装置は前記プリチャージ信号の制御手段に接続され、前記第 1 と第 2 のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第 1 の電力消費と前記第 2 の電力消費の和が所定値となされるごとく構成されたことを特徴とする情報処理装置である。

## 【0065】

第 18 の形態は、データ処理装置 A と、データ処理装置 B と、これらを接続する信号線と該信号線をプリチャージするためのプリチャージ信号線制御装置を有するマイクロコンピュータにおいて、該データ記憶装置は、該プリチャージ信号線制御装置に接続され、さらに相補的プリチャージバス制御装置にも接続され、該プリチャージバス制御装置は、該データ信号線に接続され、該相補的プリチャージバス制御装置は、充放電装置に接続され、該データ信号線での消費電力と、該充放電装置で消費される電力の和が一定になるように該データ信号線のプリチャージ直後にバスに流すデータをビット反転して該充放電装置に入力する該相補

的プリチャージバス制御装置を有することを特徴とする情報処理装置である。

## 【0066】

第19の形態は、二つのデータ処理装置A、Bと、これらを接続する信号線と該信号線をプリチャージするプリチャージ信号線制御装置とを有する情報処理装置において、信号線の途中に反転装置を有し、反転装置を挟んで、同一の配線容量を持つ正論理と負論理の信号線から構成される信号線を有することを特徴とする情報処理装置である。

## 【0067】

第20の形態は、データ処理装置Aとデータ処理装置Bとこれらを結ぶ信号線とを有する情報処理装置において、信号線とデータ処理装置Bのデータを暗号化するための暗号化装置、復号化装置をデータ処理装置Aと信号線との間に有する事を特徴とする情報処理装置である。

## 【0068】

第21の形態は、データ処理装置Aとデータ処理装置Bとこれらを結ぶ信号線を有する情報処理装置において、信号線とデータ処理装置B内のデータを暗号化・復号化するための暗号化・復号化装置をデータ処理装置Aと信号線との間およびデータ処理装置Bと信号線の間有する事を特徴とする情報処理装置である。

## 【0069】

以下は、わけても本願の情報記憶装置に関する主な発明の諸形態である。

## 【0070】

第21の形態は、データ処理装置と情報記憶装置と、これらを結ぶ信号線を有する情報処理装置において、データ処理装置と信号線の間暗号化装置を有し、信号線と情報記憶装置との間に復号化装置を有することを特徴とした、情報処理装置である。

## 【0071】

第22の形態は、複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別し、記録・読み出しが可能な情報記憶装置において、情報を格納する際に情報を暗号化する暗号化装置と、情報を読み出す際の復号化装置とを有する事を特徴とする情報記憶装置である。



【0072】

第23の形態は、データ処理装置と、情報をあらかじめ暗号化して記憶している情報記憶装置と、情報記憶装置とデータ処理装置を結ぶ信号線と、暗号化された情報を複号化する複号化装置とを有することを特徴とした、情報処理装置である。

【0073】

第24の形態は、記憶装置と、記憶装置を含むデータ処理装置と、それらを結ぶ信号線に接続され、記憶装置と記憶装置を含むデータ処理装置との間の情報転送を制御する情報転送制御装置において、転送元の情報が格納された番地を記憶するためのアドレスレジスタと、転送先の番地を記憶するためのアドレスレジスタと、転送する情報の数をカウントするための数値を格納するカウンタと、カウンタの値をデクリメントするための演算回路と、記憶装置間で転送するデータを一時的に保存するデータバッファと、アドレスレジスタの値を更新するための演算回路と、転送アドレスの転送順番をランダム化する回路を有することを特徴とする情報転送制御装置である。

【0074】

以上、本願発明の関する主な発明の諸形態を説明したが、更に、本願発明においては、前記充放電装置として、データを配送する信号線と同等の配線容量を持つダミー信号線を有することものを用いることが出来る。更には、前記充放電装置として、データを配送する信号線と同等のプリチャージダミー信号線を有することものを用いることが出来る。

【0075】

また、鍵情報を用いる形態は、起動時に暗号化に用いる鍵情報を自動的に設定する暗号化キー自動設定装置を用いることが出来る。あるいは、鍵情報を用いる形態は、暗号化に用いる鍵情報を定期的に自動再設定する暗号化キー自動再設定装置を用いることが出来る。

【0076】

また、暗号化の鍵情報の一部として、記憶装置の番地情報を用いる暗号化・複号化装置を用いることが出来る。更には、暗号化複号化装置として、暗号化の鍵

情報を設定・変更する手段を有する暗号化複号化装置としても良い。

【0077】

また、本願発明の情報処理装置は、暗号化に用いた鍵情報及び暗号化の方式などの複号化に必要な暗号情報を記憶する領域を有するデータ処理装置Bと、データ処理装置B内に記憶された暗号情報に基づいて複号化を行う複号化装置を用いて構成することが出来る。また、暗号化・複号化装置として、記憶装置を複数の領域に分割し、領域ごとに暗号化の有無を指定するための暗号化領域指定装置を有し、暗号化するか否かを記憶装置の領域に応じて指定可能な暗号化・複号化装置を用いて構成することが出来る。また、暗号化・複号化装置として、特定のデータパターンに対しては暗号化を行わない暗号化・複号化装置を用いて構成することが出来る。

【0078】

また、本願発明の情報処理装置は、起動時に暗号化に用いる鍵情報を自動的に設定する暗号化キー自動設定装置を用いて構成することが出来る。更には、暗号化に用いる鍵情報を定期的に自動再設定する暗号化キー自動再設定装置を用いて構成することが出来る。

【0079】

また、本願発明の情報処理装置は、複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別し、記録・読み出しが可能な情報記憶装置において、情報を格納する際に情報を暗号化する暗号化装置と、情報を読み出す際の複号化装置とを用いることが出来る。更には、暗号化・複号化装置の暗号化鍵を自動的に初期化する暗号化鍵自動設定装置を用いることが出来る。また、本願発明の情報処理装置は、暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする暗号化領域判定装置を用いることが出来る。

【0080】

【発明の実施の形態】

図5は発明の第1の実施の形態を説明する為の情報処理装置の概要を説明する

基本構成図である。勿論、図5は情報処理装置の当該発明に係わる部分の主要部のみを例示している。当該情報処理装置の他の部分は通例の構成を用いて十分である。

## 【0081】

本実施の形態の例の情報処理装置は、データ処理装置A (ROM) 0101 (Read Only Memory: リード・オンリー・メモリ) とデータ処理装置B (CPU) 0102 (Central Processing Unit: 中央処理装置) とが信号線 (バスライン) 0113 にて接続されている。そして、情報処理装置A側に電力発生装置C 0114 が設けられている。

## 【0082】

この電力発生装置Cの例は、排他的論理和演算装置 (EXOR) 0103、0104、インバータ0105、PMOSゲート回路0107、NMOSゲート回路0108、抵抗器R0109、コンデンサC 0110、データの一時記憶用のラッチ回路 (フリップフロップ) などを有して図のように構成されている。尚、リード・オンリー・メモリはデータ読み出し専用のメモリで、データの書き込みはできない。データの一時記憶用のラッチ回路は0111、0112を有して構成されている。

## 【0083】

尚、ここでデータ処理装置 (ROM) 等の表示は、ROMを主として構成したデータ処理装置を意味している。他の情報処理装置 (RAM) も同様である。

## 【0084】

また、この例において、抵抗器R 0109の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサC 0110の静電容量は、信号線の信号容量に等しいものとする。ここでは説明を簡単にするため、信号線のサイズは1ビットとし、CPUは8ビットプロセッサであるものとする。尚、信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0085】

まず、本願発明を用いない通例の半導体記憶装置では、信号線を介する消費電

力の観測から、半導体装置の内部情報をいかに推定できるのかを説明する。この説明によって本願発明の有効性が十分に理解されるであろう。

【0086】

データ処理装置A (ROM) 0101内に記憶されているデータをデータ処理装置B (CPU) 0102に転送する場合、これを信号線 (バスライン) 0113に乗せて転送しなければならない。

【0087】

ここに、信号線 (バスライン) 0113のデータ転送に要する消費電力を観測する観測者がいた場合、当該観測者は、本願発明に係わる電力発生装置Cがなければ、次のような事実を観測することが出来る。即ち、データが、仮に「01000101001」という並びだったとすると、0から1、1から0にビット反転するときには発生する消費電力を観測することにより、「反転、反転、未反転、未反転、反転、反転、反転、反転、未反転、反転」という事がわかる。

【0088】

この消費電力の観測結果に基づく「反転と未反転」のデータ列は、当該データ列の直前のデータビットの値によって次の2つの状態であることが判明する。即ち、前記データの直前のデータビットの値が不明である場合、次の2つの状態である。

【0089】

(1) 直前のデータが0と仮定した場合、当該データ列は01000101001であることになる。

【0090】

(2) 直前のデータが1と仮定した場合、当該データ列は10111010110であることになる。

【0091】

このように、消費電力の観測による分析は、本来は2の12乗、即ち4096通りあるデータ列が、僅か上記の2通りにまで減少する。従って、極めて多く存在する情報の可能性がわずか2つの可能性まで推測され、従って、存在するのが僅か2つの可能性であれば、その可能性より内部情報を十分把握することが可能

となる。

【0092】

本願発明はこうした消費電力の分析を阻止するひとつの方策を提供するものである。

【0093】

尚、ここで、本願発明の情報処理装置の動作の説明をするに先立って、本願発明に係わる電力発生装置の例について説明する。勿論、例示する電力発生装置以外にも具体的構成を考えることは可能である。以下に事例についても同様である。

【0094】

図5で点線で囲った部分0115は、本電力発生装置の論理演算を行う回路領域を示す。符号0203と0204は排他的論理和を行う回路である。符号0205は反転回路で、「0」の入力に対しては「1」を出力する回路である。

【0095】

この回路の論理式表示は、次のようになる。

【0096】

$$R = \text{not} (CDD \text{ xor } (PBD \text{ xor } DATA))$$

この論理式の出力は前述の表1の如くなる。このことは、排他的論理和 (xor) が表2となることから、容易に理解出来る。

【0097】

尚、ここで、CDDは考察するデータ信号の直前に、充放電装置に入力されたデータ、PBDは考察するデータ信号の直前に、当該信号線に乗っているデータ、更にDATAはデータ処理装置Aから出力されたデータである。

【0098】

【表2】

X	Y	X exor Y
0	0	0
1	0	1
0	1	1
1	1	0

表2

【0099】

又、PBDあるいはCDDのデータの一時記憶方法として、図6に例示するフリップフロップをあげることが出来る。ここで、NAND（902、903、904、905）は、表3に従って出力する演算装置である。NOT（901）はビットを反転する装置で、図4におけるビット反転回路と同じものである。

【0100】

【表3】

X	NOT X
0	1
1	0

表3

【0101】

図6にデータの一時記憶用のフリップフロップ回路は、制御信号が1の時、PBDはバスのデータを出力し、制御信号が0のとき、PBDはそれ以前の値を保つ。本フリップフロップ回路のより具体的な使用形態は後述される。

## 【0102】

実際、制御信号をCS (Control Signal)、バスラインのデータをBUSと表示するならば、このフリップフロップ回路の動作は、次の4つの論理式で表すことが出来る。

## 【0103】

$$x = \text{BUS} \text{ nand } \text{CS}$$

$$y = (\text{not BUS}) \text{ nand } \text{CS}$$

$$\text{PBD} = x \text{ nand } \text{PBD}$$

$$z = y \text{ nand } \text{PBD}$$

今、制御信号CSが1であるとする、nandはビットを反転するから、上述の論理式は次の通りとなる。

## 【0104】

$$x = \text{not BUS}$$

$$y = \text{BUS}$$

$$z = y \text{ nand } \text{PBD}$$

$$\text{PBD} = x \text{ nand } z$$

従って、BUSが1であれば、 $0 \text{ nand } z = 1$ より、 $\text{PBD} = 1$ となる。BUSが0であれば、 $z = 0 \text{ nand } \text{PBD} = 1$ 、 $\text{PBD} = (\text{not BUS}) \text{ nand } 1 = \text{BUS} = 0$ となる。こうして、PBDはBUSと一致する。

## 【0105】

一方、制御信号が0の時は、xもyも1であるから、PBDは前の値を保持する。

## 【0106】

<本願発明の第1の実施の形態での動作>

次に本例の情報処理装置における、データ転送の処理を、図1を参酌して、具体的に説明する。

## 【0107】

ROM0101からプログラムの一部である命令[EXOR R2, R4]が信

号線 0113 を通して CPU に転送される場合を考える。これが、16 進数で、  
[CA 24] という機械語に対応するものとする。このデータは信号線に流される際、11001010001000100 というビットパターンとなる。

#### 【0108】

まず、次の初期条件を仮定して考察する。第 1 にこのデータの直前に信号線に乗ったデータが 0 であると仮定する。また、第 2 に定常消費電力発生装置 C のコンデンサは、充電状態にあるとする。即ち、この状態はデータ 1 が乗っている状態に対応する。更に、第 3 に CPU からデータがバスに乗ったということを知らせる制御信号が、ラッチ 0111、0112 に入力されるものとする。

#### 【0109】

[(1) 信号列の最初の「1」の転送=データ「0」より「1」の変換動作]

まず、最初の 1 が乗る際に、信号線 0113 は充電され、当該信号線 0113 に 1 が乗っている状態となる。このとき、同じデータが定常消費電力発生装置 C 0114 に入力される。このとき、電力発生装置 C 0114 がどのように動作するかを詳細に説明する。

#### 【0110】

CPU からデータ 1 は排他的論理和演算装置 0103 に入力される。同時に、CPU からデータの出力信号を受けて、ラッチ回路 0112 は、保持していた信号線 0113 に直前に乗っていた値 0 を排他的論理演算装置 0103 に入力する。このとき、排他的論理演算装置 0103 は、以下の前述の表 2 にしたがって演算を行うので、0 と 1 の排他的論理和は 1 となる。この値が、排他的論理和演算装置 0104 に入力される。

#### 【0111】

CPU からデータの出力信号を受けて、ラッチ回路 0111 は、保持しているコンデンサ 0110 のデータ（電荷）1 を排他的論理和演算装置 0104 に入力するので、排他的論理和演算装置 0104 は、表 2 にしたがって、0 を出力する。この値は、インバータ 0105 に入力され、前述の表 3 にしたがって値 1 を出力する。



## 【0112】

この1という値が、PMOSゲート0107に入力される。PMOSは、ゲート電圧がLOWのときのみ通電するので、この場合は通電しない。一方、インバータ0105から出力された値1は、NMOSゲート0108に入力されている。これにより、ゲート0108が通電し、コンデンサ0111が放電を行う。これによって信号線0113とコンデンサ0111における電力消費量の和は信号線を1本充電したときと同じになる。

## 【0113】

## 〔(2) データが「1」より「1」への変換動作〕

次のデータは、1で、直前の信号線0113のデータも1である。コンデンサは充電状態である。このときの定常消費電力発生装置の動作は以下のようになる。

## 【0114】

まず、情報処理装置B(CPU)0102からのデータ1が乗る際は、信号線0113は既に充電状態にあり、信号線0113は充電されない。このとき、同じデータが定常消費電力発生装置C0114に入力される。情報処理装置B(CPU)0102からのデータ1は排他的論理和演算装置0104に入力される。同時に、情報処理装置B(CPU)0102からデータの出力信号を受けて、ラッチ回路0112は、保持していた信号線0113に直前に乗っていた値1を排他的論理演算装置0103に入力する。このとき、排他的論理演算装置0103は、表2にしたがって演算を行うので、1と1の排他的論理和は、0となる。この値が、排他的論理和演算装置0104に入力される。

## 【0115】

情報処理装置B(CPU)0102からのデータの出力信号を受けて、ラッチ回路0111は、保持しているコンデンサ0110のデータ(電荷)1を排他的論理和演算装置0104に入力するので、排他的論理和演算装置0104は、表2にしたがって、1を出力する。この値は、インバータ0105に入力され、表3にしたがって値0を出力する。

## 【0116】

この0という値が、PMOSゲート0107に入力される。このPMOSは、ゲート電圧がLowのときのみ通電する。従って、この場合は通電状態になり、Vddが供給され、コンデンサ0110が充電される。一方、インバータ0105から出力された値0は、NMOSゲート0108に入力されている。これにより、このNMOSゲート0108が通電しない。ここでコンデンサ0110は1ビット分の電力を消費し、これによって信号線0113とコンデンサ0110における電力消費量の和は信号線を1本充電したときと同じになる。

## 【0117】

## 〔(3) データが「1」より「0」への変換動作〕

次のデータは、0である。信号線0113のデータは1であり、コンデンサ0110は放電した状態にある。このときの電力発生装置0114の動作は次のようになる。

## 【0118】

まず、情報処理装置B(CPU)0102からのデータ0が乗る際は、信号線0113は充電状態にあるので、信号線0113では放電が行われる。信号線0113上の電荷は放電によって1ビット分の電力を消費する。このとき、同じデータ0が定常消費電力発生装置C0114に入力される。情報処理装置B(CPU)0102からのデータ0は排他的論理和演算装置0103に入力される。同時に、情報処理装置B(CPU)0102からデータの出力信号を受けて、ラッチ回路0112は、保持していた信号線0113に直前に乗っていた値1を排他的論理演算装置0103に入力する。このとき、排他的論理演算装置0103は、表2にしたがって演算を行うので、0と1の排他的論理和は、1となる。この値が、排他的論理和演算装置0104に入力される。

## 【0119】

情報処理装置B(CPU)0102からのデータの出力信号を受けて、ラッチ回路0111は、保持しているコンデンサ0110のデータ(電荷)0を排他的論理和演算装置0104に入力するので、排他的論理和演算装置0104は、表2にしたがって、1を出力する。この値は、インバータ0105に入力され、表

3にしたがって値0を出力する。

【0120】

この0という値が、PMOSゲート0107に入力される。このPMOSは、ゲート電圧がLowのときのみ通電する。従って、この場合は通電状態になり、Vddが供給され、コンデンサ0110の充電が行われる。一方、インバータ0105から出力された値0は、NMOSゲート0108に入力されている。これにより、このNMOSゲート0108が通電しない。これによって信号線0113とコンデンサ0110における電力消費量の和は信号線を1本充電したときと同じになる。

【0121】

以下、全く同様の流れで、表1の全ての場合を導くことができる。図7の(b)は、先の命令コード「1100101000100100」に対するデータの流れとコンデンサの状態を示している。

【0122】

このようにして、全てのパターンについて、信号線0113とコンデンサ0110の消費電力の和は、信号線0113の1ビット充放電において消費される電力と同じである。従って、デバイスの消費電力を調べることによって信号線0113に乗ったデータを推測することが困難となる。

【0123】

こうして製造された情報処理装置を内蔵する半導体集積回路装置を、カード部材に適用して、高セキュリティのカード部材を提供することが出来る。カード部材における半導体集積回路装置の配置は、図2に示したものと基本的に同様である。カード部材としては接触型と非接触型があるが、本願発明はいずれの方式にも当然適用することが出来る。

【0124】

そして、前記チップはこれらの信号を外部から、即ち、例えば端末機から、供給されることによって稼動する。

【0125】

尚、前記端末機自体は基本的に通例のカード・システムのものを用いて十分で

ある。以下、簡単にカード・システムの動作を例示する。図3はこのカード・システムの概念を例示する。

【0126】

ICカード52の中にはチップ51があって、リーダライタ53とデータのやりとりを行う例を示している。リーダライタのなかには、コントロールプロセッサ54およびデータベースとなる磁気ディスク55などが存在する。まず、リーダライタ53からICカード52に対して、IDの問い合わせが行われる。まず、リーダライタ53からICカード52に対して、ID (IDENTIFICATION)、例えば、当該カードの管理責任者を特定する為の氏名コードまたは認識コードの問い合わせが行われる。図3にはこの状態を(1)として示した。この氏名コードまたは認識コードはICチップの中にある所定のエリアに格納されている。ICカードは氏名コードをリーダライタに返答する。図3にはこの状態を(2)として示した。リーダライタはデータベース53にある氏名コードを検索して、データベース上の鍵コードを獲得する。

【0127】

リーダライタは乱数をICカードに送る。この乱数は、例えばリーダライタ内のMPUで回路的に発生される。LAN等でサーバ側から乱数を供給することも出来る。ICカードは、乱数を受け取った時点で、コマンドによってリーダライタから指示を受け、乱数を鍵コード発生部に従って発生した鍵コードによって暗号化した乱数を作成する。

【0128】

一方、リーダライタはICカードと同様にデータベースから得た鍵コードを使用して、ICカードへ送ったのと同じ乱数を暗号化する。これによって得られた暗号化された乱数の結果と先のICカードからの暗号化された乱数を照合して、一致がとれれば、ICカードとリーダライタの相互認識が完了して、ICカードの正当性が認められる。

【0129】

このようにして、本システムでは、この鍵コードがリーダライタに伝えられるとリーダライタは磁気ディスクの中のIDを検索して、正しく登録された鍵コー

ドによるIDであると認識する。

【0130】

生成されたICカードの鍵コード(IDコード)は、氏名コードまたは認識コードとともにデータベースに格納される。

【0131】

生成された鍵コードは電子マネーとしてICカードが使用される時の本人認証や偽造チェックやICカードとリーダライタの相互認証に使用することが出来る。

【0132】

上記システムは、例えば、一般商店での支払や、チケットの購入、定期券での改札、免許証のチェック、テレフォンカードによる電話等々多くの分野に応用することが出来る。

【0133】

以上のようなカード部材ならびにカード・システムは、以下に述べる発明の諸形態を用いて実施可能なことは言うまでもない。

【0134】

続いて、本願発明に係わる情報処理装置の実施の諸形態を説明する。

【0135】

図8は発明の第2の実施の形態を説明する為の情報処理装置の概要の基本構成図である。本例は、情報処理装置間の信号の伝達が双方向に行われ、且つ電力発生装置を双方の情報処理装置に共有して設けられた例である。

【0136】

本実施例の情報処理装置では、情報処理装置A(CPU)0201と情報処理装置B(RAM)0202(Pandom Access Memory:データの読み書きができるメモリ)とが信号線(バスライン)0213によってつながれている。そして、情報処理装置A(CPU)0201と情報処理装置B(RAM)0202に対して電力発生装置C0114が設けられている。

【0137】

電力発生装置C0114は、排他的論理和演算装置(EXOR)0203、02

04、インバータ0205、NMOSゲート回路0207、PMOSゲート回路0208、抵抗器R0209、コンデンサC0210、データの一時記憶用のラッチ回路（フリップフロップ）0211、0212を有する。ここで、抵抗器R0209の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサC0210の静電容量は、信号線の信号容量に等しいものとする。ここでは簡単のため、信号線のサイズは1ビットとし、CPUは8ビットプロセッサであるものとする。尚、信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分である。

## 【0138】

本実施の形態においては、前述の情報処理装置の第1の実施の形態の構成を一部そのまま用いている。特に、情報処理装置A(CPU)0201から、情報処理装置B(RAM)0202にデータを信号線0213によって転送する場合は、第1の実施の形態の情報処理装置の例におけるROMから、RAMにデータを転送する際の定常消費電力発生装置の動作と全く同じ動作を行う。

## 【0139】

本例において特徴的なのは、情報処理装置間の信号の伝達が双方向に行われることである。即ち、それは、第1の実施の形態の情報処理装置の例のように一方的なデータ転送ではなく、情報処理装置A(CPU)0201から情報処理装置B(RAM)0202へのデータ転送だけでなく、情報処理装置B(RAM)0202から情報処理装置A(CPU)0201へのデータ転送も行うということである。

## 【0140】

従って、これに伴って定常消費電力発生装置0114が、その双方のデータ転送に際してその機能を果たすように接続されている。

## 【0141】

本例においては、情報処理装置A(CPU)0201が、情報処理装置B(RAM)0202に対してデータの読み出し信号を送り、それを受けて情報処理装置B(RAM)0202がデータを信号線0213に乗せると同時に、排他的論理和演算装置0203にもデータを送信する。これ以後の動作は、第1の実施の形態の情報処理装置の例において、情報処理装置A(ROM)0101から、情報処

理装置B (CPU) 0102にデータを転送する際の定常消費電力発生装置0114の動作と全く同じである。従って、その動作の詳細説明は省略する。

#### 【0142】

図8においては、情報処理装置A (CPU) 0201と定常消費電力発生装置C 0114との距離が、情報処理装置B (RAM) 0202と定常消費電力発生装置C 0114との間の距離よりも短く図示されている。しかし、実際の構成では、ほぼ同じ距離に位置させ、情報処理装置A (CPU) 0201あるいは情報処理装置B (CPU) 0202と定常消費電力発生装置C 0114とのデータのやりとりを行う信号線は、情報処理装置A (CPU) 0201あるいは情報処理装置B (CPU) 0202と信号線0213との間の信号線よりも短いものとする。このとき、消費電力を調べることによって、信号線0213に乗ったデータを推測することが困難となる。

#### 【0143】

図9は発明の第2の実施の形態の変形例を説明する為の情報処理装置の基本構成図である。本例は、情報処理装置間の信号の伝達が双方向に行われ、且つ電力発生装置が双方の情報処理装置に対応して設けられた例である。

#### 【0144】

本実施例の情報処理装置は、情報処理装置A (CPU) 0251、情報処理装置B (RAM) 0252が信号線 (バスライン) 0263によってつながれている。そして、前記双方の情報処理装置に対して電力発生装置C 0115、および電力発生装置D 0116が配されている。

#### 【0145】

電力発生装置C 0115は、排他的論理和演算装置 (EXOR) 0253、0254、インバータ0255、PMOSゲート回路0257、NMOSゲート回路0258、抵抗器R 0259、コンデンサC 0260、データの一時記憶用のラッチ回路 (フリップフロップ) 0261、0262を有して構成される。電力発生装置Dは、排他的論理和演算装置 (EXOR) 0264、0265、インバータ 0266、PMOSゲート回路0268、NMOSゲート回路0269、抵抗器R 0270、コンデンサC 0271、データの一時記憶用のラッチ回路 (フ

リップフロップ) 0272、0273を有して構成される。

【0146】

次に、次の条件を仮定してその動作を考察する。抵抗器R0259の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサC0260の静電容量は、信号線の信号容量に等しいものとする。

【0147】

ここでは簡単のため、信号線のサイズは1ビットとし、CPUは8ビットプロセッサであるものとする。尚、信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分である。

【0148】

本例においては、第1の実施の形態の情報処理装置の例の構成を一部そのまま用いている。特に、情報処理装置A(CPU)0251から、情報処理装置B(RAM)0252にデータを信号線0263によって転送する場合は、第1の実施の形態の情報処理装置の例において、情報処理装置A(ROM)0101から、情報処理装置B(CPU)0102にデータを転送する際の定常消費電力発生装置の動作と全く同じ動作を行う。従って、その詳細説明は省略する。

【0149】

本例で特徴的なのは、第1の実施の形態における情報処理装置の実施例のように一方的なデータ転送ではなく、情報処理装置間の信号の伝達が双方向に行われることである。即ち、この例では、情報処理装置A(CPU)0251から情報処理装置B(RAM)0252へのデータ転送だけでなく、情報処理装置B(RAM)0252から情報処理装置A(CPU)0251へのデータ転送も行う。本実施例においては、情報処理装置A(CPU)0251が、情報処理装置B(RAM)0252に対してデータの読み出し信号を送り、それを受けて情報処理装置B(RAM)0252がデータを信号線0263に乗せると同時に、定常消費電力発生装置D0116における、排他的論理和演算装置0264にもデータを送信する。定常消費電力発生装置D0116は、定常消費電力発生装置C0115と同一のものである。そして、これ以後の動作は、第1の実施の形態における情報処理装



置の実施例において、情報処理装置A (ROM) 0101から、情報処理装置B (CPU) 0102にデータを転送する際の定常消費電力発生装置の動作と全く同じである。このとき、消費電力を調べることによって信号線0263に乗ったデータを推測することが困難となる。

## 【0150】

図10は発明の第3の実施の形態を説明する為の情報処理装置の基本構成図である。

## 【0151】

本実施例の基本的構造は、第1の実施の形態と同様である。本例は、ダミー信号線を用いる例である。即ち、本例では、第1の実施の形態に例示した抵抗器0109とコンデンサ0110の部分が、ダミー信号線0309に置き換えられている。

## 【0152】

本実施例の情報処理装置は、データ処理装置A (ROM) 0301とデータ処理装置B (CPU) 0302とが信号線 (バスライン) 0312でつながれている。そして、データ処理装置A (ROM) 0301に対して、電力発生装置C 0117が設けられている。電力発生装置C 0117は、排他的論理和演算装置 (EXOR) 0303、0304、インバータ0305、PMOSゲート回路0307、NMOSゲート回路0308、ダミー信号線0309、データの一時記憶用のラッチ回路 (フリップフロップ) 0310、0311を有して構成される。

## 【0153】

ここで、ダミー信号線0309の静電容量は、信号線0312の静電容量に等しいものとし、抵抗値は、信号線0312のそれと実質的に同じであるものとする。即ち、ダミー信号線0309は信号線0312と全く同一の信号線を用いると考えてよい。ここでは説明を簡単にするため、信号線のサイズは1ビットとし、CPUは8ビットプロセッサであるものとする。尚、信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0154】

本例では、前記ダミー信号線0309の静電容量が、第1の実施の形態に例示した抵抗器0109とコンデンサ0110の部分と同等の役割を果たす。従って、本例の動作は基本的に第1の実施の形態における情報処理装置の実施の形態と同様である。従って、その詳細説明は省略する。

## 【0155】

図11は発明の第4の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ電力発生装置を有する例である。

## 【0156】

本実施例の情報処理装置は、データ処理装置A (ROM) 0401とデータ処理装置B (CPU) 0402が信号線0408によってつながれている。そして、電力発生装置C0118がデータ処理装置A (ROM) 0401側に設けられている。そして、本例は、プリチャージ方式の制御であるので、プリチャージ信号線制御装置0407を有している。

## 【0157】

プリチャージ信号線制御装置0407は、二つのPMOSゲート回路0409、0410を有し、そのゲート部には、データ処理装置B (CPU) 0402からのデータ制御信号が入力される。ソース側には、Vddが接続されており、データ処理装置B (CPU) 0402からの制御信号に応じて信号線0408及び電力発生装置C0118にVddを供給する。電力発生装置C0118は、NMOSゲート回路0404、抵抗器(R) 0405、コンデンサC0406、論理積演算回路0411を有する。ここで、抵抗器R0405の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサC0406の静電容量は、信号線の信号容量に等しいものとする。ここでは説明を簡単にのため、信号線のサイズは1ビットであるものとし、CPUは8ビットプロセッサであるとする。信号線のサイズは、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0158】

データ処理装置A (ROM) 0401内に記憶されているデータをデータ処理装置B (CPU) 0402に転送する場合、データ信号を信号線 (バスライン) 0408に乗せて転送しなければならない。

## 【0159】

ここで、信号線 (バスライン) 0408のデータ転送に要する消費電力を観測する観測者がいた場合を考えてみる。今、データが、仮に「01000101001」という並びだったとする。そして、定常電力発生装置C0118がない場合、プリチャージ信号線制御装置0407の働きによって、前記のデータ値が0から1に変化するときが発生する消費電力を観測することにより、このデータ列が、「01000101001」であることが直接わかる。尚、ここでは、正論理で考えるものとした。すなわち、信号線の電位がLOWのとき、データ値は、0であり、HIGHのときにデータ値1に対応する。勿論、負論理の場合にも同じようにデータ値が1から0に変化するときが発生する消費電力を観測することにより、データ列を推測することが出来る。

## 【0160】

本願発明はこうした消費電力の分析を阻止するひとつの方策を提供するものである。本例のデータ転送の処理は次の通りである。

## 【0161】

ROM0401からプログラムの一部である命令 [EXOR R2, R4] が信号線0408を通してデータ処理装置B (CPU) 0402に転送される場合を考える。これが、16進数で、[CA 24] という機械語に対応するものとする。このデータは信号線に流される際、「1100101000100100」というビットパターンとなる。

## 【0162】

データ処理装置B (CPU) 0402が制御信号を発信すると、プリチャージ信号線制御装置0407の二つのPMOS0409、0410のゲートが通電してVddを信号線0408に供給して1 (HIGH) にクリアする。更に、当該電位は、電力発生装置C0118のコンデンサ0406を充電する。まず、最初

のデータ (MD-DATA) 1 が乗る際に、信号線の放電が行われ、電力が消費される。このとき、同じデータ (MD-DATA) 1 と MACK 信号が電力発生装置 C 0 1 1 8 に入力される。

## 【0163】

このとき、定常電力発生装置 C 0 1 1 8 がどのように動作するかを詳細に述べる。

## 【0164】

前記のデータ列の最初の値「1」の場合、データ処理装置 A (ROM) 0 4 0 1 からのデータ (MD-DATA) 1 が準備される。この最初の値「1」の準備によって、データ処理装置 A (ROM) 0 4 0 1 は MACK 信号を出力する。MACK 信号は、出力が確定すると 1 であり、確定していない状態では 0 となる。MACK 信号が論理積演算装置 0 4 1 1 に入力され、同時にデータ (MD-DATA) 1 が、信号線 0 4 0 8 に乗る。そして、さらに、データ (MD-DATA) 1 は論理積演算装置 0 4 1 1 に入力される。

## 【0165】

MD-DATA、MACK 信号が共に 1 であるから、論理積演算装置 0 4 1 1 の出力は 1 である。そして、この値は、NMOS ゲート回路 0 4 0 4 に入力される。NMOS ゲート回路 0 4 0 4 は、入力 1 (HIGH) に対しては通電するので、コンデンサ 0 4 0 6 は放電を行う。一方、信号線 0 4 0 8 上の値は変化しないので、信号線 0 4 0 8 での充放電は行われない。

## 【0166】

充放電を行なわない信号線 0 4 0 8 においては電力消費はなく、一方、放電を行なうコンデンサ 0 4 0 6 では電力の消費がなされる。従って、その両者の和は、信号線 1 本の充電で消費される消費電力に等しい。

## 【0167】

次に、前記のデータ列の第 2 の値「1」の場合、データ 1 が信号線 0 4 0 7 に乗る。このときには既に信号線 0 4 0 7 はプリチャージされ 1 にクリアされているので、再び上で説明したのと同じ動作が行われ、信号線 0 4 0 8 における消費電力と、コンデンサ 0 4 0 6 における消費電力の和は、信号線一本の充電で消費

される消費電力に等しい。

【0168】

次に、前記のデータ列の第3の値「0」の場合、データ(MD-DATA)0が信号線0408に乗る。このときは、既に信号線0408はプリチャージされ1にクリアされているので、値「1」から「0」への変化に伴って電力消費が行われる。MD-DATA0とMACK信号1は、論理積演算装置0411に入力される。論理積演算装置0411の出力値は0となり、この値は、NMOSゲート回路0404に入力される。NMOSゲート回路0404は、入力0(LOW)に対しては通電しないので、コンデンサ0406での電力消費は行われない。

【0169】

データ値「1」から「0」への変化がある前記信号線では電力の消費があり、一方、コンデンサ0406では電力の消費がない。従って、その両者の消費電力の和は、信号線1本の充電で消費される消費電力に等しい。

【0170】

以下同様の動作を行うので、常に信号線0408における消費電力と、コンデンサ0406における消費電力の和は、信号線一本の充電で消費される消費電力に等しい。

【0171】

上述の信号線0408でのデータ「1100101000100100」に対するコンデンサ0406の状態を、相互に対応させて図7の(a)に示す。

【0172】

図12は発明の第5の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ電力発生装置としていわゆるダミー信号線を用いた例である。

【0173】

本実施例の基本的構造は、第4の実施の形態と同様であって、抵抗器とコンデンサの部分が、ダミー信号線に置き換えられただけである。本実施例の情報処理装置は、データ処理装置A(ROM)0501、データ処理装置B(CPU)0502、プリチャージ信号線制御装置0505、信号線(バスライン)0506

、定常電力発生装置C0119を有する。ここで、ダミー信号線0507の静電容量は、信号線0506の静電容量に等しいものとし、抵抗値は、信号線0506のそれと同じであるものとする。即ち、ダミー信号線0507と信号線0506とは実質的に同一の信号線を用いる。尚、定常電力発生装置C0119は、NMOSゲート回路0504、ダミー信号線0507、論理積演算装置0503を有する。

## 【0174】

ここでは簡単のため、信号線のサイズは1ビットとし、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0175】

動作は基本的に前述の第1の実施の形態の情報処理装置の実施例と同様である。従って、その詳細説明は省略する。

## 【0176】

図13は発明の第6の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ反転装置を有する例である。

## 【0177】

本実施例の情報処理装置は、データ処理装置A(CPU)5001とデータ処理装置B(RAM)5002とが、各々信号線5007、5006につながれている。そして、両信号線5007と5006の間に反転装置5003が設けられている。更に、本例はプリチャージ信号線制御装置5008を有する。

## 【0178】

反転装置5003は、4つのCMOSインバータ5004、5005、5009、5010、PMOSゲート回路5011、5013、NMOSゲート回路5014、5012を有して構成されている。尚、信号線5006と信号線5007の静電容量並びに抵抗値は実質的に同一であるものとする。

【0179】

データ処理装置A (CPU) 5001から、データ処理装置B (RAM) 5002にデータを転送する際、データ処理装置A (CPU) 5001は、制御信号をプリチャージバス制御装置5008に発信する。この信号によって、プリチャージバス制御装置5008内のPMOSゲート及びNMOSゲートを通電する。そして、電位V<sub>dd</sub>が信号線5007、5006を充電してHIGHの状態にする。更に、データ処理装置A (CPU) 5001からの制御信号がインバータ5010、NMOSゲート回路5012に入力され、PMOSゲート回路5011、NMOSゲート回路5012が通電状態になる。この後、データ処理装置A (CPU) 5001からデータが送信される。

【0180】

データ処理装置A (CPU) 5001からのデータが0のとき、信号線5007が放電する。この値はインバータ5004によって1に変換され、信号線5006に信号を送る。しかし、前述の通り、既に信号線5006は充電されているので充放電は起きない。そして、この値1がデータ処理装置B (RAM) 5002に入力される。この値「1」は、データ処理装置A (CPU) 5001が送ったデータ「0」とは反転している。

【0181】

逆にデータ処理装置A (CPU) 5001からのデータが、1であった場合は、信号線5007では充放電が起きず、信号線5006で放電が生ずる。データ処理装置B (RAM) 5002からデータ処理装置A (CPU) 5001にデータが送られる場合も同様である。信号線5006と信号線5007の静電容量並びに抵抗値は実質的に同一であるから、全ての場合において、信号線5006、5007での充放電の総和は信号線5006あるいは5007の充放電で生ずる電力が消費され、総和は一定となる。

【0182】

次に、第7の実施の形態より第22の実施の形態の諸形態は、信号線に乗せるデータを暗号化する諸例である。

## 【0183】

図14は発明の第7の実施の形態を説明する為の情報処理装置の基本構成図である。本例は暗号化装置を用いて信号線に乗せるデータの暗号化を図る基本的な例である。

## 【0184】

本実施例の情報処理装置は、データ処理装置A（CPU）0601とデータ処理装置B（RAM）0602とが信号線（バスライン）0605によってつながれている。そして、データ処理装置A（CPU）0601と信号線（バスライン）0605との間に暗号化装置および復号化装置を有する。本例の暗号化装置としては排他的論理和演算装置0603及び、復号化装置としては排他的論理和演算装置0604が用いられている。尚、こうした暗号化装置および復号化装置として他の構成の諸装置を用いることが出来ることは言うまでもない。

## 【0185】

ここでは説明を容易にするのため、信号線0605のサイズは8ビットとし、データ処理装置A（CPU）0601は8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

又、ここでは、信号線0605の制御方式はスタティック信号線制御方式であるとして説明する。尚、本実施の形態の思想の効果は、プリチャージ信号線制御方式においても同じである。

## 【0186】

本例の暗号化装置は、固定された8ビットの鍵（Key）とCPUからの8ビットのデータとのビット毎の排他的論理演算装置である。一方、本例の復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算装置である。尚、鍵（Key）自体は通例の技術で十分である。

## 【0187】

第1の発明の実施の形態の実施例で述べたように、スタティック信号線制御方式の場合は、信号線に直前に乗っていた値とのビット反転数に比例して電力消費が行われる。以下、1ビットに対する消費電力をPと表示する。



## 【0188】

例えば、データ処理装置A (CPU) 0601からデータ「0110100」を送信したとする。信号線0605に直前に乗っていたデータが、「11010101」であるとする、ビット反転数は5である。従って、この信号線0605で消費される電力は5Pである。

## 【0189】

データ処理装置A (CPU) 0601から、データ「10110111」を信号線0605を通してデータ処理装置B (RAM) 0602に転送し、これを再び、データ処理装置B (RAM) 0602よりデータ処理装置A (CPU) 0601に戻す過程を考える。この場合、信号線0605に直前に乗っていたデータは、「00010101」であると仮定する。又、鍵 (Key) は、「10101110」であるものとする。

## 【0190】

暗号化装置、復号化装置がない場合、信号線のデータは、「00010101」より「10110111」と変化する。従って、この場合、ビット反転数3に対応して、消費電力は3Pである。

## 【0191】

しかし、本例の場合、暗号化装置、即ち排他的論理和演算装置0603の働きにより、信号線0605に乗るデータは、鍵 (Key) 「10101110」と情報処理装置A (CPU) 0601からのデータ「10110111」とのビット毎の排他的論理和となる。即ち、その結果は「00011001」である。

## 【0192】

このとき、信号線0605のデータは、信号線0605に直前に乗っていたデータ「00010101」より前述の排他的論理和の出力「00011001」に変化することとなる。従って、この場合は、ビット反転数2に対応して、電力消費は2Pとなる。この電力消費は、暗号化装置、復号化装置がなく、本来消費されるはずの3Pとは異なる値である。

## 【0193】

データ処理装置B (RAM) 0602には、暗号化された値「0001100

1」が格納される。この暗号化された値を再び信号線 0605 を通してデータ処理装置 A (CPU) 0601 に返す時を考察してみる。

【0194】

データ処理装置 B (RAM) 0602 より信号線 0605 に出力されるデータは、「00011001」より「00011001」となって変化しない。従って、信号線 0605 は充放電せず、電力消費は行われぬ。

【0195】

この信号線 0605 よりの値は、復号化装置、即ち、排他的論理和演算装置 0604 の働きにより、信号線 0605 よりのデータ「00011001」と鍵「10101110」との排他的論理和「10110111」がデータ処理装置 A (CPU) 0601 に入力される。同一の数の排他的論理和は、0 になるので、データ処理装置 A (CPU) は矛盾なく演算が可能である。しかも信号線 0605 での充放電による消費電力は、本来のデータとは異なる。従って、消費電力を基礎として、元のデータを推測することが困難となる。

図 15 は発明の第 8 の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例であるが、更に、暗号化あるいは復号化する際、鍵 (Key) として乱数を用いる例である。本例では、データ処理装置より伝達するデータと乱数を用いて暗号化をはかり、一方、データ処理装置に伝達されるデータと前記と同様の乱数を用いて復号化を図るのである。

【0196】

本実施例の情報処理装置は、データ処理装置 A (CPU) 0701 とデータ処理装置 B (RAM) 0702 とが信号線 (バスライン) 0705 でつながれている。データ処理装置 A (CPU) 0701 と信号線 0705 の間に暗号化装置および復号化装置を有する。暗号化装置としては排他的論理和演算装置 0703 及び、復号化装置としては排他的論理和演算装置 0704 が用いられる。

【0197】

そして、これらの暗号化装置および復号化装置に対する鍵として、乱数を用いる例である。従って、本例は乱数発生装置 (RNG) 0706、および暗号化装

置 0703 および復号化装置 0708 への鍵バッファ 0707、0708 が準備されている。乱数発生装置自体等は通例のものを用いて十分である。

【0198】

乱数発生装置 0706 は、情報処理装置起動時のリセット信号 (Reset) を受けて稼動し、8ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファ 0707、0708 は、前述の 8ビットの乱数を格納するもので、8つのフリップフロップを有して構成されている。

【0199】

ここでは説明のため、信号線 0705 のサイズは 8ビットとし、CPU は 8ビットプロセッサであるものとする。信号線のサイズ、CPU のビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、信号線 0705 の制御方式はスタティック信号線制御方式であるものとする。尚、本実施の形態の効果はプリチャージ信号線制御方式においても同じである。

【0200】

暗号化装置 0703 は、固定された 8ビットの鍵 (Key) とデータ処理装置 A (CPU) 0701 からの 8ビットのデータとのビット毎の排他的論理演算を行なう装置である。又、復号化装置 0704 も同じ鍵とデータとのビット毎の排他的論理和演算を行なう装置である。

【0201】

リセット時に乱数生成装置 0706 を起動させて新たな 8ビット鍵を設定する部分を除いて本実施例は、本発明の第 6 の実施の形態の実施例と同じで良い。従って、鍵バッファに乱数の鍵が設定されて以後の動作も第 6 の実施の形態の実施例と基本的に同様である。従って信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することがより困難となる。

【0202】

図 16 は発明の第 9 の実施の形態を説明する為の情報処理装置の基本構成図で

ある。本例は信号線に乗せるデータの暗号化を図る別な例であり、更に暗号化装置が暗号鍵自動設定装置を有する例である。本例は特に暗号化の鍵情報の提供源に特徴がある。

## 【0203】

本実施例の情報処理装置は、データ処理装置A (CPU) 0801とデータ処理装置B (RAM) 0802とがデータ信号線0806によってつながれている。暗号化装置としての排他的論理和演算装置0803、復号化装置としての排他的論理和演算装置0804、そして、鍵バッファ0805が設けられている。更に、データ処理装置A (CPU) 0801とデータ処理装置B (RAM) 0802とに対してアドレス信号線上位4ビット0807、アドレス信号線下位4ビット0808が設けられる。

## 【0204】

ここでは説明のため、データ信号線0806のサイズは8ビットとし、アドレス信号線0807、0808のサイズも同じ8ビットであり、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、データ信号線0806及びアドレス信号線0807、0808の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

## 【0205】

暗号化装置0803は、固定された8ビットの鍵 (Key) とデータ処理装置A (CPU) 0801からの8ビットのデータとのビット毎の排他的論理演算を行なう装置である。復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算を行なう装置である。鍵バッファ0805の上位4ビットは固定された鍵であり、下位4ビットは、アドレス信号線の下位4ビットが格納されるものとする。図16の鍵バッファ0805にこの旨を図示している。以下、鍵の固定部分の4ビットは、D (16進数表現) であるものとする。

## 【0206】

データ処理装置A (CPU) 0801がデータ処理装置B (RAM) 0802

のあるアドレスにデータを転送する場合を考える。今、データ処理装置 B (RAM) 0802 は、アドレス F0 からアドレス FF までとする。尚、ここで、この値は本質的ではない。

【0207】

データ処理装置 A (CPU) 0801 は、表 4 に示す以下のデータを、アドレス F4 から順に転送する。

【0208】

【表 4】

A d d r e s s	CPUからのデータ
F4	5D
F5	A0
F6	FE

表 4

【0209】

データ処理装置 A (CPU) 0801 からデータ 5D が転送される直前にデータ信号線 0806 に乗っていたデータは、CF であるとする。データ 5D の転送が行われると、アドレス信号線には、F4 が乗り、データ処理装置 B (RAM) 0802 の転送位置が確定する。

【0210】

データ 5D は、排他的論理和演算装置 0803 に入り、固定鍵 4 ビット D (16 進数表現) と、アドレス F4 の下位 4 ビットの 4 との排他的論理和  $5D \oplus D4 = 01011101 \oplus 11010100$  (2 進数表現) = 10001001 (2 進数表現) = 89 (16 進数表現) が送信される。即ち、[固定鍵 4 ビット / アドレス下位 4 ビット] と [データ上位 4 ビット / データ下位 4 ビット] のビット毎の排他的論理和演算を行うことによって暗号化が行われた上で送信される。

## 【0211】

この89（尚、この値は16進数表現である。）が、データ信号線0806に乗ったときに消費される電力は、3Pとなる。それは、データが、CF（11001111）より89（10001001）と変化するので、ビット反転値が3であることによる。尚、ここで用いているPは、本発明の第7の実施の形態において用いた記号である。即ち、Pは1ビットに対する消費電力である。

## 【0212】

以下同様のプロセスを経て、信号線0806に乗るデータは、CF（11001111）より89（10001001）へ、更にこの情報は75（01110101）、更に28（00101000）へと変化する。

## 【0213】

この変化に対応する信号線0805における消費電力は、3Pより6Pへ、更に2Pと変化する。

## 【0214】

これは本来の変化、CF（11001111）より5D（01011101）、更にA0（10100000）よりFE（11111110）への変化とは異なっている。、即ち消費電力の変化として見れば、3Pより7Pへ、更に5Pへの変化に対応する。従って、半導体装置の消費電力の測定から、内部のデータを推測することが困難となる。

## 【0215】

図17は発明の第10の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例であるが、更に暗号化あるいは復号化装置がその設定手段を有する例である。

## 【0216】

本実施例の情報処理装置は、データ処理装置A（CPU）0901とデータ処理装置B（RAM）0902とが信号線0907によってつながれている。本例は、暗号化装置としての排他的論理和演算装置0903、復号化装置としての排他的論理和演算装置0904を有し、且つ8ビットの鍵データを保持する鍵バッファ0905を有する。ここでは説明のため、信号線0907のサイズは8ビット

トとし、データ処理装置A (CPU) 0901は8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0217】

また、鍵バッファ0905は、データ処理装置A (CPU) 0901に接続されている。そして、この鍵バッファ0905に、データ処理装置A (CPU) 0901から書き込みを行うことができ、且つこの鍵バッファ0905はデータ処理装置B (RAM) 0902からの出力データの暗号化、入力データの復号化に用いられる。データ処理装置A (CPU) 0901から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第6の実施の形態における実施例と同様である。従って、その詳細説明は省略する。

## 【0218】

ここで前述の鍵バッファ0905の具体的な例を図40に例示する。尚、ここに例示した鍵バッファは、例えば、以下に本願発明の実施の形態として例示する図25、図28および図29などの鍵バッファ、1607、1406、1407、1607の実装例として適宜用い得ることは言うまでもない。

## 【0219】

図40を用いて上述の鍵バッファを説明する。本例は、1ビットのシフトレジスタ1461、1462、1463、1464、1465、1466、1467、および1468、1ビットの排他的論理和演算装置1470、1471、1472、および乱数発生装置 (RNG) 1469からなる。

## 【0220】

シフトレジスタ1461、1462、1463、1464、1465、1466、1467、および1468には、初期ビットが格納されているものとする。ここでは、説明のため、順に並べたとき10101110となるものとしておく。一回のビットシフトを行う度に乱数発生装置1469は1ビットの乱数を発生するものとする。乱数は1ビットずつ発生し、例えば、011となったとする。この時、この鍵バッファが発生する8ビット値の列は、以下のようになる。

【0221】

10101110 --> 01011100 --> 10111101 --> 011  
11111

この8ビットの振る舞いは、非常に乱数に近いことが知られている。一般に、正しい乱数の発生には時間がかかることが多い。しかし、本例のそれは、1ビットの乱数を用いるだけで、8ビットの（疑似）乱数列を生成することができる。従って、本例の乱数発生の手段によって、極めて高速な処理が可能となる。このように高速動作の疑似乱数発生手段によって、極めて実用的な情報処理装置を提供することが出来る。

【0222】

図18は発明の第11の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。更に、本例は鍵選択装置（マルチプレクサ）を用いて鍵（Key）を選択する例である。

【0223】

本実施例の情報処理装置は、データ処理装置A（CPU）1001とデータ処理装置B（RAM）1002とがデータ信号線1009でつながれている。暗号化装置として排他的論理和演算装置1003、復号化装置として排他的論理和演算装置1004が用いられる。

【0224】

鍵選択装置（マルチプレクサ）1006、1014、鍵テーブル1007、1015、鍵バッファ1008、1013、鍵番号転送用信号線1010を有する。尚、前記鍵テーブル1007、1015は固定されたもので、書き換えできないものとする。そして、鍵テーブル1007、1015にはKey0とKey1が格納されている。勿論、本願発明において、鍵テーブルとして書き換え可能な鍵テーブルを用いることも可能である。鍵選択装置1006は鍵バッファ1008に接続され、暗号化装置1003に対して用いられる。鍵選択装置1014は鍵バッファ1013に接続され、復号化装置1004に対して用いられる。鍵番号転送用信号線1010によって鍵番号が転送される。



【0225】

ここでは説明を容易にするのため、信号線1009のサイズは8ビットとし、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【0226】

本例によれば、ユーザ（例えばICカードのアプリケーションを制作する企業）は、鍵テーブル1007のどの鍵を用いて暗号化するのかを、鍵選択ビットバッファ1011に指定することで選択できる。以下、鍵選択ビットバッファ1011に格納された値をSKEYBITと呼ぶ。

【0227】

鍵選択装置1006は、鍵選択ビットバッファ1011に格納されたSKEYBITを参照して、鍵テーブル1007中から用いるべきKeyを取り出し、鍵バッファ1008に格納する。ここで、SKEYBITが0であれば、鍵選択装置（マルチプレクサ）1006は、鍵テーブル1007のKey0を選択し、鍵バッファ1008に格納し、もしSKEYBITが1であれば、鍵テーブル1007のKey1を選択し、鍵バッファ1008に格納する。

【0228】

データ処理装置A（CPU）1001が、データ処理装置B（RAM）1002にデータを転送する際、排他的論理和演算装置1003によって鍵バッファ1011に格納されている8ビットの鍵データとデータ処理装置A（CPU）1001からの8ビットのデータとの排他的論理和がとられる。そして、この値がデータ信号線1010に乗せられて、データ処理装置B（RAM）1002に転送される。同時に、鍵選択ビットバッファ1011に格納されているSKEYBITの値を鍵番号転送用信号線1010を通してデータ処理装置B（RAM）1002に転送される。このとき、データ処理装置B（RAM）1002内のデータは、表5に示される形で格納される。

【0229】

【表5】

SKEYBIT (1bit)	DATA(8bit)
-------------------	------------

表5

【0230】

これは、DATAが、鍵番号がSKEYBITとなる鍵によって暗号化されていることを示している。鍵選択ビットバッファ1011内のSKEYBITがプログラム等によって書き換えられた場合は、別の鍵によって暗号化される。例えば、データ処理装置B(RAM)の内部データは、次のようなものになる。

【0231】

1 EF  
0 A3  
1 3E  
1 54  
0 3D

これらのデータを、再びデータ処理装置A(CPU)1001に戻して用いるときには、次の動作を行なう。これら暗号化データを転送する前に、データ処理装置B(RAM)1002より、鍵番号転送用信号線1010を通して鍵選択ビットを鍵選択装置1014に転送する。鍵選択装置1014は、鍵選択ビットに応じて鍵テーブル1015に格納された鍵を選択し、鍵バッファ1013に転送する。その上でデータ処理装置A(CPU)1001は、データ処理装置B(RAM)1002に対してデータを要求し、データ処理装置B(RAM)1002の該当データをデータ信号線1009に乗せる。更に、排他的論理和演算装置1004によって該当データと鍵バッファ1013に格納された鍵との排他的論理和を取り、データ処理装置A(CPU)1001に入力する。データの暗号化に

用いた鍵番号に応じて復号化が行われるので、データ処理装置 A (CPU) 1001 では矛盾なく処理が行われる。

### 【0232】

図 19 は発明の第 12 の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は、信号線のデータを暗号化して伝達するひとつの例である。更には、本例は記憶装置を複数の領域に分割し、領域毎に暗号化するか否かを指定して、暗号化、復号化する方法である。

### 【0233】

本実施例の情報処理装置は、データ処理装置 51101 と情報記憶装置 51102 とがデータバス 51107 によってつながれている。データ処理装置 51101 に暗号化装置 51103 および復号化装置 51104 が設けられている。そして、本例では、暗号化判定回路 7312 によって暗号するか否かを判定して、この情報を暗号化装置 51103 および復号化装置 51104 に与えられる。この動作の為、暗号鍵記憶装置 51106、暗号化領域指定レジスタ 7311、暗号化判定回路 7312、AND 回路 51112 などが設けられている。更に、本例は情報記憶装置とデータ処理装置の間にはアドレスバス 51108 を有する。

### 【0234】

ここで、情報記憶装置 51102 自体の構成は、通例に従って十分である。情報記憶装置の記憶領域は、記憶領域のアドレス値によって複数の領域に分類され、それぞれの領域に対して暗号化を行うか否かを、暗号化領域指定レジスタ 7311 で指定する。暗号化判定回路 7312 は、アドレスバス 51108 に現れるアドレス値と、暗号化領域指定レジスタ 7311 の値によって、暗号化を行うか判定する。

### 【0235】

図 20 は、暗号化判定回路のひとつの実施例を示す。この暗号化判定回路の例では、メモリを分割する際の上位  $p$  ビット分を参照し、メモリアレイの領域を  $p$  ビットのそれぞれの状態で識別し、 $2^p$  の領域に分割する。暗号化領域指定レジスタ 7311 は、 $2^p$  ビットの長さを持ち、各ビットはメモリアレイ上の 1 つの領域と対応し、暗号化を行うか否かを制御する。

## 【0236】

暗号化領域指定レジスタ7311の各ビットと、該ビットに相当するアドレス領域を表すビットパターンに対して、ビットがすべて1となるようにNOTを挟んだのち、暗号化領域指定レジスタの該当ビットとの論理積をとる。この論理積が1のときは、暗号化を行い、0の時は暗号化を行わない。暗号化領域指定レジスタ7311の各ビットに対して同様の回路を作り、その後論理積すべてのビットの論理和を論理和演算装置7314で取る。この論理和が1のときは、暗号化を行い、0の時は暗号化を行わないようにする。

## 【0237】

暗号化判定回路7312の出力は、暗号鍵とのANDが論理積演算装置51112で計算され、暗号化装置51103複号化装置51104にそれぞれ送られる。論理積演算装置51112の出力は、暗号化を行う際には、暗号鍵と同じ値になるが、暗号化を行わないときには、0となる。暗号化装置51103は、暗号鍵として0が与えられると、入力と出力が等しくなるので、暗号化を行わないのと等価になる。

## 【0238】

読み出し時の複号化の手順は、書き込みと同様、アドレスの値と暗号化領域指定レジスタ7311の値によって、複号化を行う際の暗号鍵を0とするか暗号鍵の値にするかを制御し、複号化を行う。

## 【0239】

このようにして、情報記憶装置をアドレスによって複数領域に分割して、それぞれの領域ごとに暗号化の有無が設定できる。暗号化を施された領域では、データバス51107に現れるビットパターンや情報記憶装置に記録されるデータのビットパターンは実際のデータとは異なるため、情報記憶装置へのデータの書き込み・読み込み時の消費電流パターンやバスで消費される電流パターンから実際のデータを推測する事が困難となる。

## 【0240】

図21は発明の第13の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化複号化を図る別な

例である。本例は特定のデータパターンに対しては暗号化を行わない例である。

【0241】

本実施例の情報処理装置は、データ処理装置A (CPU) 1101とデータ処理装置B (RAM) 1102とが信号線1109でつながれている。暗号化装置としては排他的論理和演算装置1103、復号化装置としては排他的論理和演算装置1104が設けられている。この暗号化装置および復号化装置に対する鍵選択の為にラッチ回路1105、8ビットの暗号化禁止データバッファ1106、復号化禁止データバッファ1113、鍵テーブル1107、1112、鍵選択装置1108、1111、など設けられている。

【0242】

ここで、復号化禁止データバッファ1113の内部のデータは、暗号化禁止データバッファ1106内部のデータと同じデータが格納されている。また、鍵テーブル1107と1112とは全く同じ鍵データが格納されている。

【0243】

ここでは説明のため、信号線0705のサイズは8ビットとし、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【0244】

鍵テーブル1107には、暗号化用の鍵 (Key) 及び、0が格納されているものとする。暗号化禁止データバッファ1106及び、復号化禁止データバッファ1113には、禁止データ (FDATA) 及び、FDATAと暗号化鍵 (Key) との排他的論理和の値が格納されている。このFDATAとKeyの排他的論理和の値をCO-FDATAと呼ぶ。CO-FDATAが必要な理由は、次のようである。データとKeyとの排他的論理和がFDATAに一致してしまった場合、この暗号化データをデータ処理装置B (RAM) 1102からデータ処理装置A (CPU) 1101に戻したときに、暗号化がなされたままデータ処理装置A (CPU) 1101に入力され、処理が矛盾するからである。

## 【0245】

鍵 (Key) との排他的論理和が FDATA に一致するのは、CO-FDATA だけであるから、暗号化禁止データバッファ 1106 及び復号化禁止データバッファ 1113 に格納しなければならないデータは、禁止データ (FDATA) 及び CO-FDATA だけである。

## 【0246】

データ処理装置 A (CPU) 1101 からデータ処理装置 B (RAM) 1102 に信号線 1109 を通してデータを転送する際、該データは、鍵選択装置 1108 及び、ラッチ回路 1105 に入力される。ラッチ回路 1105 は、鍵選択装置 1108 からデータ保持解除信号の値 (OUTDATA-BIT) が 1 になるまで、該データを保持し続け、OUTDATA-BIT が 1 になると、保持を解除し、排他的論理和演算装置 1103 に入力される。鍵選択装置 1108 に入力されたデータは、暗号化禁止データバッファ 1106 に保持されている 8 ビットの暗号化禁止データ (FDATA) 及び CO-FDATA と比較される。そして、鍵選択装置 1108 に入力されたデータがそのいずれか一方と同じであれば、鍵テーブル 1107 より値 0 を選択して保持し、ラッチ回路 1105 に OUTBIT-DATA 1 を送るとともに、排他的論理和演算装置 1103 に値 0 を送信する。任意のビット値  $x$  と 0 との排他的論理和が  $x$  に等しいので、このときには該データは暗号化されずに信号線 1109 に乗せられ、データ処理装置 B (RAM) に入力される。

## 【0247】

一方、FDATA または CO-FDATA と該データが同一でない場合は、鍵テーブルより値 Key を選択して保持し、ラッチ回路 1105 に OUTBIT-DATA 1 を送るとともに、排他的論理和演算装置 1103 に値 Key を送信する。このとき、該データは暗号化されて信号線 1109 に乗せられ、データ処理装置 B (RAM) に入力される。逆に情報処理装置 B (RAM) のデータをデータ処理装置 A (CPU) に転送するときには、そのまま信号線 1109 に乗せて転送を行う。このときも、以上と同様のプロセスでデータと FDATA または CO-FDATA が一致したときには復号化されず、不一致のときには同じ Key

による復号化がなされ、矛盾なく処理が行われる。

【0248】

図22は発明の第14の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータを暗号化する別な例である。更には本例はデータを伝達する両データ処理装置と信号線の間の双方に暗号化および復号化装置を挿入する例である。

【0249】

本実施例の情報処理装置は、データ処理装置A(CPU)1301とデータ処理装置B(RAM)1302とが信号線1307でつながれている。暗号化装置としては排他的論理和演算装置1303、1305、復号化装置としては排他的論理和演算装置1304、1306が用いられる。排他的論理和演算装置1303、1304、1305、1306は、全て同一の鍵Keyとデータとの排他的論理和を計算して出力するものである。データ処理装置A(CPU)1301から出力されたデータは、排他的論理和演算装置1303によって暗号化され、信号線1307を通してデータ処理装置B(RAM)1302に転送される。しかし、一方、データ処理装置B(RAM)1302に入力される前に排他的論理和演算装置1306によって復号された後、データ処理装置B(RAM)1302に入力される。

【0250】

本発明の第6の実施の形態とは異なり、本実施例においては、データ処理装置B(RAM)1302内のデータは、暗号化されていない元のデータとなる。また、データ処理装置B(RAM)1302内のデータがデータ処理装置A(CPU)1301に転送されるときには、排他的論理和演算装置1305によって暗号化が行われ、信号線1307を通してデータ処理装置A(CPU)1301に転送されるが、データ処理装置A(CPU)1301に入力される前に排他的論理和演算装置1304によって復号された後、データ処理装置A(CPU)1301に入力される。

【0251】

このとき、信号線における充放電は、本発明の第6の実施の形態における情報

処理装置におけるものと全く同じである。

【0252】

図23は発明の第15の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例はデータ処理装置と信号線の間に暗号化および復号化装置ならびに鍵情報を設定する装置を挿入する例である。

【0253】

本実施例の情報処理装置は、本発明の第6の実施の形態の情報処理装置の実施例を双方向化したものである。本例は、データ処理装置A(CPU)1401、データ処理装置B(RAM)1402、信号線1410、暗号化装置としての排他的論理和演算装置1403、1411及び、復号化装置としての排他的論理和演算装置1404、1412、乱数発生装置(RNG)1409、鍵バッファ1405、1406、1407、1408を有する。

【0254】

乱数発生装置1409は、情報処理装置起動時のリセット信号(Reset)を受けて稼動し、8ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファは、8ビットの乱数を格納するもので、8つのフリップフロップから構成される。ここでは説明のため、信号線1410のサイズは8ビットとし、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、信号線1410の制御方式はスタティック信号線制御方式であるものとする。尚、プリチャージ信号線制御方式においても本例の効果は同じである。

【0255】

リセット時に乱数生成装置1409を起動させて新たな8ビット鍵を設定する部分を除いて本実施例は、本発明の第13の実施の形態における情報処理装置と同じものである。従って、鍵バッファに乱数の鍵が設定されて以後の動作も同様である。動作の詳細説明は省略する。



## 【0256】

本例においても、当然、信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することが困難となる。

## 【0257】

図24は発明の第16の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例は暗号化に用いる鍵情報の一部として記憶装置の番地情報を用いる例である。

## 【0258】

本実施例の情報処理装置は、基本的に本発明の第7の実施の形態の情報処理装置を双方向化したものである。本例は、データ処理装置A（CPU）1501、データ処理装置B（RAM）1502、暗号化装置としての排他的論理和演算装置1503、1505、復号化装置としての排他的論理和演算装置1504、1506、鍵バッファ1507、データ信号線1510、アドレス信号線上位4ビット1508、アドレス信号線下位4ビット1509を有する。ここでは説明のため、データ信号線1510のサイズは8ビットとし、アドレス信号線1508、1509のサイズも同じ8ビットであり、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、データ信号線1510及びアドレス信号線1508、1509の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

## 【0259】

暗号化装置は、固定された8ビットの鍵（Key）とCPUからの8ビットのデータとのビット毎の排他的論理演算装置であり、復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算装置である。鍵バッファ1507の上位4ビットは固定された鍵であり、下位4ビットは、アドレス信号線下位4ビット1509のデータが格納されるものとする。

## 【0260】

データ処理装置A (CPU) からデータが転送される場合の動作は、本発明の第7の実施の形態の情報処理装置において説明したものと同一である。

## 【0261】

しかし、データ信号線1510に暗号化されたまま入力されるのではなく、鍵バッファ1507に格納されている暗号化鍵を用いて復号化されてからデータ処理装置B (RAM) 1502に入力される。逆に、データ処理装置B (RAM) 1502の内部のデータをデータ処理装置A (CPU) 1501に転送するときには、データ処理装置A (CPU) 1501から、対応するアドレスがアドレス線1508、1509によって転送され、その値を用いて鍵バッファ1507の値が決定される。そして、この鍵バッファ1507の値とデータとの排他的論理和が、データ信号線1510に乗せられる。排他的論理和演算装置1504によって、この値と暗号化に用いた鍵バッファ1507の鍵との排他的論理和をとることによって復号し、データ処理装置A (CPU) に入力される。このとき、信号線における充放電の動作は、前述の第7の実施の形態の情報処理装置の実施例におけるものと全く同一である。

## 【0262】

図25は発明の第17の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。更には本例はデータ処理装置と信号線の間に暗号化および復号化装置を挿入し、且つ暗号化に用いる鍵情報を自動的に再設定する例である。

## 【0263】

本実施例の情報処理装置は、データ処理装置A (CPU) 1601、データ処理装置B (RAM) 1602、暗号化装置としての排他的論理和演算装置1603、1605、復号化装置としての排他的論理和演算装置1604、1606、8ビットの鍵を格納する鍵バッファ1607、乱数生成装置 (RNG) 1608、5ビット入力1出力の論理和演算装置1609、5ビットの大きさを持つカウンタ1610、信号線1611から構成される。カウンタ1610は、クロック信号 (CLK) のエッジの立ち上がりに合わせてカウントを行い、5ビットより大

きな部分は無視される。ここでは説明のため、信号線 1611 のサイズは 8 ビットとし、CPU は 8 ビットプロセッサであるものとする。信号線のサイズ、CPU のビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0264】

データ処理装置 A (CPU) 1601 からデータ処理装置 B (RAM) 1602 にデータを転送する場合、データ処理装置 A (CPU) 1601 は、クロック信号に同期してデータを転送する。クロック信号が発信されると、カウンタ 1610 はカウントを始める。論理和演算装置 1609 は、カウンタの各ビット全てに対する論理和を乱数生成装置 1608 に送信する。乱数生成装置 1608 は、該論理和の値が 0 であれば、8 ビットの乱数を生成し、該 8 ビット乱数を鍵バッファ 1607 に送信して停止する。このとき、カウンタの値が全て 0 になったときのみ、乱数生成装置 1608 は、0 を受け取るので、鍵は 32 クロック毎に暗号化、復号化に用いる鍵を交換することになる。鍵バッファ 1607 は、排他的論理和演算装置 1603、1604、1605、1606 全てに同一の鍵を供給する。

## 【0265】

データ処理装置 A (CPU) からデータをデータ処理装置 B (RAM) に信号線 1611 を通して転送する際、まず、排他的論理和演算装置 1603 にて鍵バッファ 1607 の値とデータとの排他的論理和を信号線 1611 に乗せて転送する。この暗号化されたデータは、データ処理装置 B (RAM) に入る前に同じ鍵バッファ 1607 の値との排他的論理和が取られるので、復号されて元のデータ値になり、データ処理装置 B (RAM) 1602 に入力される。データ処理装置 B (RAM) 1602 のデータをデータ処理装置 A (CPU) 1601 に転送する場合も同様である。

## 【0266】

図 26 は発明の第 18 の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例はデータ処理装置 A (CPU) 1701 から鍵の書き換えを行うことが

できる例である。

【0267】

本実施例の情報処理装置は、データ処理装置A (CPU) 1701、データ処理装置B (RAM) 1702、暗号化装置としての排他的論理和演算装置1703、1705、復号化装置としての排他的論理和演算装置1704、1706、8ビットを格納する鍵バッファ1707、信号線1709から構成される。ここでは説明のため、信号線1709のサイズは8ビットとし、CPUは8ビットプロセッサであるものとする。信号線のサイズ、CPUのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【0268】

鍵バッファ1707はCPU1701に接続されており、CPU1701から鍵バッファ1707の内容を変更することが可能である。鍵バッファ1707に保持された鍵情報は、データ処理装置A (CPU) 1701からの出力データの暗号化、入力データの復号化に用いられる。データ処理装置A (CPU) 1701から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第15の実施の形態における実施例と同様である。

【0269】

図27は発明の第19の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータを暗号化し、且つ復号化してデータを格納する例である。

【0270】

本実施例の情報処理装置は、データ処理装置A (CPU) 1301、データ処理装置B (RAM) 1302、暗号化装置としての排他的論理和演算装置1303、復号化装置としての排他的論理和演算装置1306、信号線1307から構成されている。排他的論理和演算装置1303、1306は、全て同一の鍵Keyとデータとの排他的論理和を計算して出力するものである。

【0271】

データ処理装置A (CPU) 1301から出力されたデータは、排他的論理和

演算装置 1 3 0 3 によって暗号化され、信号線 1 3 0 7 を通してデータ処理装置 B (RAM) 1 3 0 2 に転送されるが、データ処理装置 B (RAM) 1 3 0 2 に入力される前に排他的論理和演算装置 1 3 0 6 によって復号された後、データ処理装置 B (RAM) 1 3 0 2 に入力される。

## 【0 2 7 2】

本発明の第 6 の実施の形態とは異なり、本実施例においては、データ処理装置 B (RAM) 1 3 0 2 内のデータは、暗号化されていない元のデータとなる。このとき、データ処理装置 A (CPU) 1 3 0 1 から、データ処理装置 B (RAM) 1 3 0 2 に送られる情報は、信号線上では暗号化されている。従って、信号線の充放電電流からは、送られた情報を推測することは困難になる。

## 【0 2 7 3】

図 2 8 は発明の第 2 0 の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は本例は信号線に乗せるデータを暗号化し、且つ復号化してデータを格納する例である。更には、本例は乱数を用いた鍵をもちいた例である。

## 【0 2 7 4】

本実施例の情報処理装置は、データ処理装置 A (CPU) 1 4 0 1、データ処理装置 B (RAM) 1 4 0 2、信号線 1 4 1 0、暗号化装置としての排他的論理和演算装置 1 4 0 3 及び、復号化装置としての排他的論理和演算装置 1 4 1 2、乱数発生装置 (RNG) 1 4 0 9、鍵バッファ 1 4 0 6、1 4 0 7 から構成される。

## 【0 2 7 5】

乱数発生装置 1 4 0 9 は、情報処理装置起動時のリセット信号 (Reset) を受けて稼動し、8 ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファは、8 ビットの乱数を格納するもので、8 つのフリップフロップから構成される。ここでは説明のため、信号線 1 4 1 0 のサイズは 8 ビットとし、CPU は 8 ビットプロセッサであるものとする。信号線のサイズ、CPU のビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

。また、信号線 1410 の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

## 【0276】

リセット時に乱数生成装置 1409 を起動させて新たな 8 ビット鍵を設定する部分を除いて本実施例は、本発明の第 19 の実施の形態における情報処理装置の実施例と同じものである。従って、鍵バッファに乱数の鍵が設定されて以後の動作も同様である。従って信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することが困難となる。

## 【0277】

図 29 は発明の第 21 の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例である。更には、本例は乱数を用いて鍵情報を設定する例である。

## 【0278】

本実施例の情報処理装置は、データ処理装置 A (CPU) 1601、データ処理装置 B (RAM) 1602、暗号化装置としての排他的論理和演算装置 1603、復号化装置としての排他的論理和演算装置 1606、8 ビットの鍵を格納する鍵バッファ 1607、乱数生成装置 (RNG) 1608、5 ビット入力 1 出力の論理和演算装置 1609、5 ビットの大きさを持つカウンタ 1610、信号線 1611 から構成される。カウンタ 1610 は、クロック信号 (CLK) のエッジの立ち上がりに合わせてカウントを行い、5 ビットより大きな部分は無視される。ここでは説明のため、信号線 1611 のサイズは 8 ビットとし、CPU は 8 ビットプロセッサであるものとする。信号線のサイズ、CPU のビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

## 【0279】

本例では、データ処理装置 A (CPU) 1601 からデータ処理装置 B (RAM) 1602 にデータを転送する場合、データ処理装置 A (CPU) 1601 は、クロック信号に同期してデータを転送する。クロック信号が発信されると、カ

ウンタ 1610 はカウントを始める。論理和演算装置 1609 は、カウンタの各ビット全てに対する論理和を乱数生成装置 1608 に送信する。乱数生成装置 1608 は、該論理和の値が 0 であれば、8 ビットの乱数を生成し、該 8 ビット乱数を鍵バッファ 1607 に送信して停止する。このとき、カウンタの値が全て 0 になったときのみ、乱数生成装置 1608 は、0 を受け取るので、鍵は 32 クロック毎に暗号化、復号化に用いる鍵を交換することになる。鍵バッファ 1607 は、排他的論理和演算装置 1603、1606 全てに同一の鍵を供給する。

## 【0280】

データ処理装置 A (CPU) からデータをデータ処理装置 B (RAM) に信号線 1611 を通して転送する際、まず、排他的論理和演算装置 1603 にて鍵バッファ 1607 の値とデータとの排他的論理和を信号線 1611 に乗せて転送する。この暗号化されたデータは、データ処理装置 B (RAM) に入る前に同じ鍵バッファ 1607 の値との排他的論理和が取られるので、復号されて元のデータ値になり、データ処理装置 B (RAM) 1602 に入力される。信号線 1611 での充放電による消費電力は、本来のデータとは異なるものであり、さらに、暗号化に用いている鍵が定期的に変化する。従って、信号線 1611 での消費電力から元のデータを推測することが困難となる。

## 【0281】

図 30 は発明の第 22 の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例である。更には、本例は鍵情報の設定、変更が出来る装置を有する例である。

## 【0282】

本実施例の情報処理装置は、データ処理装置 A (CPU)、データ処理装置 B (RAM)、暗号化装置としての排他的論理和演算装置 1703、復号化装置としての排他的論理和演算装置 1706、8 ビットを格納する鍵バッファ 1707、信号線 1709 から構成される。ここでは説明のため、信号線 1709 のサイズは 8 ビットとし、CPU は 8 ビットプロセッサであるものとする。信号線のサイズ、CPU のビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【0283】

鍵バッファ1707はデータ処理装置A (CPU) 1701に接続されており、データ処理装置A (CPU) 1701から鍵バッファ 1707の内容を変更することが可能である。鍵バッファ1707に保持された鍵情報は、データ処理装置A (CPU) 1701からデータ処理装置B (RAM) へ信号線1709を通じて送られるデータの暗号化および複号化の双方に使われる。データ処理装置A (CPU) 1701から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第19の実施の形態と同様である。従って、その動作の詳細説明は省略する。

【0284】

尚、以下の第23より第29までの発明の実施の形態はいわゆる半導体記憶装置あるいはより大きい情報処理装置に含まれる半導体記憶装置の部分に本願発明の基本思想を適用した例である。従って、以下の第23より第29までの発明の実施の形態を、例えば、いわゆるマイクロコンピュータ・システムに含まれる記憶部に適用することが出来る。更には、こうした大きな半導体装置システムの記憶部に本例の如き方法を適用し、更に、全体システムの情報の処理に際して、上記した本願諸発明を合わせて適用することも当然可能である。

【0285】

図3.1は発明の第23の実施の形態を説明する為の情報処理装置の基本構成図である。

【0286】

第23の実施例の情報記憶装置7001は、いわゆる半導体記憶装置の例である。

【0287】

本半導体記憶装置は、基本的な半導体記憶装置と同様に、メモリセルアレイ7002、アドレスデコーダ7005、およびデータバス7007を有して構成される。そして、本例は、信号の暗号化の為に、暗号化装置7003、複号化装置7004、暗号鍵記憶装置7006を有する。



## 【0288】

ここで、メモリセルアレイ 7002 の構成自体は、通例に従って十分である。メモリセルは多くの例は 1 トランジスタ、1 キャパシタンスで構成される。更にまた、その他の形態もとることが出来る。

## 【0289】

図 3 2 はメモリセルアレイ 7002 の代表的な例を示す回路図である。図 3 2 に点線で囲った領域 66 が 1 つのメモリセルに当たる領域である。各メモリセル 66 は各ビット線 65 によってそれぞれセンスアンプ 60、61 に接続される。一方、各ワード線 64 によってそれぞれワード線ドライバ 62、63 に接続されている。こうした半導体メモリ装置に対して本願発明に技術思想を適用して、セキュリティに関して極めて有用な効果を奏する。尚、図 3 2 に示したセンスアンプ 60、61 の出力は、例えば図 3 1 のメモリセルアレイ 7002 の読み出しデータとなる。一方、メモリセルアレイ 7002 の書き込みデータに従い、ビット線 66 を通して、ワード線により選択されたメモリセル 66 のキャパシタンスを充放電する。尚、以下に示すメモリセルアレイを用いた本願発明の実施の諸形態に本例のメモリセルアレイを用いて十分である。勿論、本願発明の他の実施の形態として、メモリセルアレイを他の形態のものを用い得ることは言うまでもない。

## 【0290】

以下に本例の動作の詳細を説明する。メモリアレイ 7002 へのデータの書き込みは、次のような動作である。データが、データバス 7007 より暗号化装置 7003 に送られる。そして、暗号化装置 7003 では、暗号鍵記憶装置（鍵バッファ）7006 内の情報を参照して、暗号化装置 7003 によって、データが暗号化される。一方、アドレスバス 7008 で指定されたアドレスが、アドレスデコーダ 7005 によりデコード化され、ワード選択信号としてメモリセルアレイ 7002 に送られる。メモリセルアレイでは、このコード化されたアドレスによって、データを書き込むべきメモリセルが選択される。そして、メモリセルには、暗号化処理装置 7003 により暗号化されたデータが書き込まれる。

## 【0291】

また、メモリセルアレイ7002からのデータの読み出しは、次のような動作である。アドレスバス7008で指定されたアドレスが、アドレスデコーダ7005によりデコードされ、ワード選択信号としてメモリセルアレイ7002に送られる。そして、ワード選択信号によって選択されたメモリセルの内容が読み出される。読み出されたメモリセルの内容は、複号化装置7004に送られる。複号化装置7004は、暗号鍵格納装置（鍵バッファ）7006より取り出した暗号鍵情報を参照して、複号化する。こうして、複号化されたデータはデータバス7007に出力する。尚、ここで、暗号鍵記憶装置7006の鍵情報は、その外部より書き換えることが出来る。本願明細書における本実施例以外の例における暗号鍵記憶装置に関しても同様のことが言える。

## 【0292】

このようにこの発明のひとつの実施例では、データバス7007から送られてきたデータをメモリセルアレイ7002に格納する前に暗号化が施され、メモリセルアレイ7002からデータを読み出す際には複号化が施されてデータバス7007に出力される。

## 【0293】

従って、メモリセルアレイを含む半導体装置においても、これまで説明してきた諸情報処理装置と同等に扱える。この結果、メモリセル上に実際に記録されるデータのビットパターンは、記憶させようとしたデータとは異なるため、セル上のデータの書き込み・読み込み時の消費電流パターンからセル上のデータを推測する事が困難になる。

## 【0294】

このように、通例のメモリセルを有する半導体記憶装置に対しても、本願の発明諸思想を適用することが出来る。本例ならびに以下の諸例に限らないことは言うまでもない。尚、上述の例では、一般的なマトリクス状のメモリアレーの行の選択についてのアドレスを言及した。しかし、当該メモリアレーの列に対して本例の発明思想を適用することが出来る。更に、メモリアレーの行列の双方に本願の発明思想を適用することも出来る。

【0 2 9 5】

これを背景として、以下の実施の諸形態において、いわゆる半導体記憶装置を情報処理装置と称する。従って、本願明細書において、情報処理装置はいわゆる半導体記憶装置をも含むものである。

【0 2 9 6】

図 3 3 は発明の第 2 4 の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化鍵を用いる。

【0 2 9 7】

本実施例の情報記憶装置は、通例の半導体記憶装置と同様に、メモリセルアレイ 7 0 0 2、アドレスデコーダ 7 0 0 5 およびデータバス 7 0 0 7 を有する。そして、本例は、信号の暗号化および復号化の為、暗号化装置 7 0 0 3、復号化装置 7 0 0 4、暗号鍵記憶装置 7 0 0 6、暗号鍵記憶装置の鍵と、アドレス情報の一部から新たな暗号化鍵を生成するための E O R 回路 7 1 0 9 を有する。ここで、メモリセルアレイ 7 0 0 2 の構成は、通例に従って十分である。

【0 2 9 8】

メモリアレイ 7 0 0 2 へのデータの書き込みは、次のような動作である。

【0 2 9 9】

データが、データバス 7 0 0 7 より暗号鍵記憶装置 7 0 0 6 に送られる。そして、暗号鍵記憶装置 7 0 0 6 では、暗号鍵記憶装置 7 0 0 6 内の情報とアドレスバス 7 0 0 8 の情報を排他的論理和演算装置 7 1 0 9 で合成する。こうして得られる暗号鍵を用いて、データバス 7 0 0 7 から送られたデータは暗号化装置 7 0 0 3 によって暗号化される。一方、アドレスバス 7 0 0 8 で指定されたアドレスが、アドレスデコーダ 7 0 0 5 によりコード化され、ワード選択信号としてメモリセルアレイ 7 0 0 2 に送られる。

【0 3 0 0】

メモリセルアレイでは、このコード化されたアドレスによって、データを書き込むべきメモリセルが選択される。こうして、メモリセルには、暗号化処理装置 7 0 0 3 により暗号化されたデータが書き込まれる。

## 【0301】

また、メモリセルアレイからのデータの読み込みは、次のような動作である。アドレスバス7008で指定されたアドレスが、アドレスデコーダ7005によりでコードされ、ワード選択信号としてメモリセルアレイ7002に送られる。そして、ワード選択信号によって選択されたメモリセルの内容が読み出される。読み出されたメモリセルの内容は、複号化装置7004に送られる。複号化装置7004は、暗号鍵記憶装置（鍵バッファ）7006内の情報とアドレスバス7008の情報を、EOR回路7109で合成して得られる暗号鍵を用いて、メモリセルから読み出された内容を複号化する。こうして、複号化されたデータはデータバス7007に出力する。

## 【0302】

このように、データバス7007から送られてきたデータをメモリセルアレイ7002に格納する前に暗号化が施され、一方、メモリセルアレイからデータを読み出す際には複号化が施されてデータバス7007に出力される。従って、半導体記憶装置は普通の情報記憶装置と同等に扱える。この結果、セル上に記録されるデータのビットパターンは記憶させようとしたデータとは異なるため、セル上のデータの書き込み・読み込み時の消費電流パターンからセル上の実際のデータが容易に推測する事が困難になる。

## 【0303】

図34は発明の第25の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化鍵を用いるが、この暗号化鍵を自動初期化するものである。

## 【0304】

本実施例の情報記憶装置は、図31の実施例の暗号鍵記憶装置7006に、暗号化鍵自動初期化装置7210を接続し、この暗号化鍵自動初期化装置7210で暗号鍵を初期化するようにしたものである。本例のその他の構成は前述の例と同様であるので、その詳細説明は省略する。

## 【0305】

暗号化鍵自動初期化装置7210は、通例の乱数発生装置を使用して、初期値

を設定する構成になっている。情報処理装置が起動もしくはリセットスタートした際に、暗号化鍵自動初期化装置 7210 は、乱数により暗号鍵を自動生成し、暗号鍵記憶装置 7006 に暗号鍵を設定する。このことにより、起動もしくはリセットスタートのたびに暗号鍵が変更され、同一のデータを格納した場合でも、起動毎にセル上のデータの書き込み、読み込み時の消費電流パターンが変化する。従って、消費電流パターンからセル上の実際のデータが容易に推測する事が困難になる。

### 【0306】

図 35 は発明の第 26 の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化を行うか否かを制御を行なうものである。

### 【0307】

本実施例の情報記憶装置は、メモリアルレイ 7002、アドレスデコーダ 7005、暗号化装置 7003、複号化装置 7004、暗号鍵記憶装置 7006、暗号化領域指定レジスタ 7311、暗号化判定回路 7312 を有する。ここで、メモリアルレイ 7002 の構成は、通例に従って十分である。

### 【0308】

メモリアルレイ 7002 はアドレス値によって複数の領域に分類され、それぞれの領域に対して暗号化を行うか否かを、暗号化領域指定レジスタ 7311 で指定する。暗号化判定回路 7312 は、アドレスバス 7008 に現れるアドレス値と、暗号化領域指定レジスタ 7311 の値によって、暗号化を行うか判定する。

### 【0309】

図 20 に、本例で用いる暗号化判定回路のひとつの実施例を示す。この例は前述したものと同様である。この暗号化判定回路の実施例では、メモリを分割する際の上位  $p$  ビット分を参照し、メモリアルレイの領域を  $p$  ビットのそれぞれの状態で識別し、 $2^p$  の領域に分割する。暗号化領域指定レジスタ 7311 は、 $2^p$  ビットの長さを持ち、各ビットはメモリアルレイ上の 1 つの領域と対応し、暗号化を行うか否かを制御する。

## 【0 3 1 0】

暗号化領域指定レジスタ 7 3 1 1 の各ビットと、当該ビットに相当するアドレス領域を表すビットパターンに対して、ビットがすべて 1 となるように NOT を挟んだのち、暗号化領域指定レジスタの該当ビットとの論理積をとる。この論理積が 1 のときは、暗号化を行い、0 の時は暗号化を行わない。暗号化領域指定レジスタ 7 3 1 1 の各ビットに対して同様の回路を作り、その後論理積すべてのビットの論理和を OR 回路 7 3 1 4 で取る。この論理和が 1 のときは、暗号化を行い、0 の時は暗号化を行わないようにする。

## 【0 3 1 1】

つぎに、暗号化判定回路 7 3 1 2 の出力と、暗号鍵の AND を論理積演算装置 7 3 1 3 で論理積を計算する。論理積演算装置 7 3 1 3 の出力は、暗号化を行う際には、暗号鍵と同じ値になるが、暗号化を行わないときには、0 を出力する。暗号化装置 7 0 0 3 は、暗号鍵として 0 が与えられると、入力と出力が等しくなるので、暗号化を行わないのと等価になる。

## 【0 3 1 2】

読み出し事の複号化の手順は、書き込みと同様、アドレスの値と暗号化領域指定レジスタ 7 3 1 1 の値によって、複号化を行う際の暗号鍵を 0 とするか暗号鍵の値にするかを制御し、複号化を行う。

## 【0 3 1 3】

このようにして、メモリセルアレイをアドレスによって複数領域に分割して、それぞれの領域ごとに暗号化の有無が設定できる。暗号化を施された領域では、セル上に記録されるデータのビットパターンは記憶させようとしたデータとは異なるため、セル上のデータの書き込み、読み込み時の消費電流パターンからセル上の実際のデータが容易に推測する事が困難になる。

## 【0 3 1 4】

第 2 7 の実施の形態より第 2 8 の実施の形態はいわゆる半導体記憶装置とその他の情報処理装置を一つの装置内に有する例である。

## 【0 3 1 5】

図 3 6 は発明の第 2 7 の実施の形態を説明する為の情報処理装置の基本構成図

である。

【0316】

本例では、情報記憶装置 7052 には予め暗号化されたデータが格納されているものとして、これ以降の動作を説明する。尚、この暗号化されたデータの格納は、これまでに説明した諸方法によって行うことが出来る。本実施例の情報記憶装置は、データ処理装置 7051、情報記憶装置 7052 がデータバス 7057 でつながれている。そして、データ処理装置 7051 とデータバス 7057 の間に複号化装置 7053 および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ 7056 が設けられている。

【0317】

ここで、複号化装置、鍵バッファ自体はこれまで説明したもので十分である。

【0318】

尚、前述したように、情報記憶装置 7052 には、複号化装置 7053 と鍵バッファ 7056 に格納された暗号化鍵により復号できる形式で暗号化された情報が予め格納されている。暗号化された情報は、データバス 7057 により複号化装置 7053 に送られ、複号化装置 7053 により複号化される。そして、復号化されたデータが複号化装置 7053 よりデータ処理装置 7051 に送られる。

【0319】

従って、情報記憶装置や信号線を流れる情報は、データ処理装置で使用される情報とは異なるビットパターンを有しており、情報記憶装置 7052 やデータバス 7057 での消費電流パターンから情報を推測する事が困難となる。

【0320】

図 37 は発明の第 28 の実施の形態を説明する為の情報処理装置の基本構成図である。本例はデータの復号化に当って、暗号化鍵を用いる例である。

【0321】

本例では、情報記憶装置 7052 には予め暗号化されたデータが格納されているものとして、これ以降の動作を説明する。尚、この暗号化されたデータの格納は、これまでに説明した諸方法によって行うことが出来る。本実施例の情報記憶装置は、データ処理装置 7051、情報記憶装置 7052 がデータバス 705

7でつながれている。そして、データ処理装置7051とデータバス7057の間に複号化装置7053および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ7056、およびアドレスバス7058が設けられている。ここで、複号化装置、鍵バッファ自体はこれまで説明したもので十分である。

#### 【0322】

複号化装置7053は、複号化する際の暗号化鍵として、情報記憶装置7052の格納アドレスの一部分と、鍵バッファ7056に格納された暗号鍵とのEORを計算したものを暗号化鍵として使用する。情報記憶装置7052には、複号化装置7053により復号可能な形式で暗号化された情報が予め格納されている。

#### 【0323】

データ処理装置7051がアドレスバス7058にアドレス情報を出力すると、情報格納装置7052は、データバスに暗号化された状態のデータをそのままデータバス7057に出力する。複号化装置7053には、情報記憶装置7052の格納アドレスの一部分と、鍵バッファ7056に格納された暗号鍵とのEORをEOR回路7054により計算された複号化鍵が暗号化された情報とが、鍵として送られる。そして、この鍵によって、データバス7057上の情報を複号化して、データ処理装置7051へ送る。

#### 【0324】

この場合、情報記憶装置7052やデータバス7057を流れる情報は、データ処理装置7051で使用される情報とは異なるビットパターンを有している。又、格納アドレスごとに暗号化の鍵情報が異なるため、消費電力が同じ値であっても、アドレスによって異なるビットパターンに暗号化されている。この為、情報記憶装置や信号線での消費電流パターンから情報を推測する事が前記第27の実施の形態に係る発明よりも更に困難となる。図38は発明の第29の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置とその他の情報処理装置を有する例である。

#### 【0325】

本実施例の情報記憶装置は、データ処理装置7051、情報記憶装置7052



がデータバス 7057 でつながれている。そして、データ処理装置 7051 とデータバス 7057 の間に複号化装置 7053 および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ 7056、およびアドレスバス 7058 が設けられている。更に、記憶領域のどの領域のデータを暗号化するかを指定する為に、AND 回路 1112、暗号化領域指定レジスタ 7311、暗号化判定回路 7312 を有する。ここで、情報記憶装置 7052 の構成は、通例に従って十分である。又、複号化装置、鍵バッファ自体など個別の手段は、例えばこれまで説明したもので十分である。

## 【0326】

本実施の形態に特徴的な暗号化領域の指定に関する動作を主に説明する。

## 【0327】

それぞれの記憶領域に対して暗号化を行ったか否かを、暗号化領域指定レジスタ 7311 で指定する。暗号化判定回路 7312 は、アドレスバス 7058 に現れるアドレス値と、暗号化領域指定レジスタ 7311 の値によって、複号化を行うか判定する。暗号化判定回路の構成は、前述の図 20 と同一である。情報記憶装置 7052 には、複号化装置 7053 により複号可能な形式で暗号化された情報が予め格納されている。データ処理装置 7051 がアドレスバス 7058 にアドレス情報を出力すると、情報格納装置 7052 は、データバスに暗号化された状態のデータを出力する。暗号化判定回路 7312 は、アドレスバス 7058 に出力されたアドレス値の一部と、暗号化領域指定レジスタ 7311 の値を参照して、該アドレスのデータが暗号化されているか否かを判定し、暗号化されている場合は 1 を、暗号化されていない場合は 0 を返す。

## 【0328】

暗号化判定回路 7312 の出力は、AND 回路 1112 にて鍵バッファ 7056 と AND が取られる。その結果、複号化装置 7053 には、暗号化されているアドレス領域をアクセスした場合は、鍵バッファ 7056 の内容が渡り、暗号化されていないアドレス領域をアクセスした場合は、0 が渡る。複号化装置 7053 は EOR 回路になっているため、0 が渡されると入力された値をそのままデータ処理装置 7051 へ渡す。したがって、暗号化された領域のデータは鍵バッファ

ァ7056の値を用いて正しく複号化される一方、暗号化されていない領域のデータはそのままデータ処理装置7051に渡される。暗号化を施された領域では、データバス7057に現れるビットパターンや情報記憶装置7052に記録されるデータのビットパターンは実際のデータとは異なるため、情報記憶装置7052の読み込み時の消費電流パターンやデータバス7057で消費される電流パターンから実際のデータを推測する事が困難となる。

## 【0329】

図39は発明の第30の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置とその他の情報処理装置を有する半導体装置システムの例である。

## 【0330】

本実施例のランダム転送制御装置は、転送元のアドレスを記憶するアドレスレジスタ18002と、転送先のアドレスを記憶するアドレスレジスタ18003と、転送元、転送先レジスタを切り替えるためのマルチプレクサ18004と、転送先、転送元アドレスレジスタの値を更新するための加算器18005と、アドレスレジスタと乱数とEORを取り、転送アドレスの転送順番をランダム化するための排他的論理和演算装置18007と、排他的論理和演算装置18007で転送順番を変えるための排他的論理和演算に用いる乱数値を生成するための乱数発生装置18006と、転送回数をカウントするためのカウンタ18009と、順番を変えて生成されたアドレスを一時的に保管するアドレスバッファ18008と、転送されるデータを一時的に保管するデータバッファ18011、転送順番をランダムかしたときのアドレスを保存するアドレスレジスタ、これらの各回路を制御して転送を実行する制御回路18012とにより構成されている。まず転送元アドレスが転送元アドレスレジスタ18002に、転送先アドレスが転送先アドレスレジスタ18003に、転送バイト数がカウンタ18009にセットされる。ここで、カウンタにセットされる転送バイト数の初期値は2の累乗の値をとる。転送元アドレスレジスタ18002転送先アドレスレジスタ18003、に初期値としてセットされる値は、転送バイト数で余剰を計算したときに、0となる値である必要がある。次に、制御装置18012の転送動作を順を追っ

て説明する。

【0331】

STEP 0 : まず制御回路 18012 から乱数発生回路 18006 へ乱数発生要求が送られ、乱数発生回路 18006 では、転送前に転送バイト数よりも小さな値の乱数を生成し保持する。

【0332】

STEP 1 : つぎに、制御回路 8012 からマルチプレクサ 18004 に対して、転送元アドレスレジスタ 18002 を選択するように選択信号が送られ、マルチプレクサをとった転送元アドレスは、乱数発生回路 18006 に保持された乱数値との排他的論理和演算を排他的論理和演算装置 18007 で行い、アドレスバッファ 18008 に格納される。

【0333】

STEP 2 : 制御回路 18012 は、アドレスバッファ 18008 のアドレス値をアドレスバスに出力し、アドレスバス 18032 に乗ったアドレス値の内容がデータバス 18031 に載ったのち、制御回路 18012 は、ラッチ信号をデータバッファ 18011 に送って、データバッファ 18011 にデータバスの値を格納する。加算回路 18005 では、転送元アドレスレジスタの値に 1 を加算する計算が行われている。加算が終わったら、制御回路 18012 から転送元アドレスレジスタに対するラッチ信号を制御して、転送元アドレスレジスタに加算回路の出力を格納する。

【0334】

STEP 3 : つぎに、制御回路 18012 は制御回路 18012 からマルチプレクサ 18004 に対して、転送先アドレスレジスタ 18003 を選択するように選択信号が送られ、マルチプレクサをとった転送先アドレスは、乱数発生回路 18006 に保持された乱数値との EOR 演算を EOR 回路 18007 で行い、アドレスバッファ 18008 に格納される。

【0335】

STEP 4 : 制御回路 18012 は、アドレスバッファ 18008 のアドレス値をアドレスバス 18032 へ、データバッファ 18011 のデータ値をデータ

バス 18031 に出力するように制御信号を送る。さらにアドレスバス 18032 のアドレスに、データバス 18031 上のデータを書き込むように制御信号を発行する。

【0336】

STEP 5: 加算回路 18005 では、転送先アドレスレジスタの値に 1 を加算する計算が行われている。加算が終わったら、制御回路 18012 は転送先アドレスレジスタ 18003 に対するラッチ信号を制御して、転送先アドレスレジスタ 18003 に加算回路 18005 の出力を格納する。

【0337】

STEP 6: カウンタ 18009 の値に -1 を加算回路 18010 で加算し、1 減算する。制御回路 18012 は、カウンタ 18009 へラッチ信号を送り、加算回路 18010 の演算結果をカウンタ 18009 に格納する。

【0338】

STEP 7: つぎに制御回路は、カウンタ 18009 の内容が 0 か否かを検査し、非ゼロの場合は、STEP 1 からの処理を繰り返す。

【0339】

以上の動作により、乱数値の違いにより、同一の内容を同一のアドレスに対して転送する場合でも、乱数発生回路で生成される乱数値が異なることで、データの転送順が異なり、動作時の消費電流パターンが毎転送ごとに異なることとなり、消費電流パターンから同一のデータを転送しているか否かを推測する事が困難になる。

【0340】

【発明の効果】

本願発明は、高いセキュリティを持つ情報処理装置を提供することが出来る。本願発明は、高いセキュリティを持つ情報記憶装置を提供することが出来る。更には、本願発明は、高いセキュリティを持つカード部材、および情報処理システムを提供することが出来る。

【図面の簡単な説明】

【図 1】

図 1 はマイクロコンピュータの基本構成を示す図である。

【図 2】

図 2 は IC カードにおける半導体集積回路装置の配置を示す図である。

【図 3】

図 3 はカード・システムの概要を示す構成図である。

【図 4】

図 4 は通例の IC カード用半導体装置における 1 サイクルの消費電力を示す電流波形を示す図である。

【図 5】

図 5 は本願情報処理装置の第 1 の実施の形態を示す基本構成図である。

【図 6】

図 6 はデータの一時記憶の為のフリップフロップの例を示す図である。

【図 7】

図 7 は信号線の状態と電力消費の為のコンデンサの状態を示す図であり、同図の (a) はプリチャージ方式の場合、同図の (b) はスタティック方式の場合の諸例を示すものである。

【図 8】

図 8 は本願情報処理装置の第 2 の実施の形態を示す基本構成図である。

【図 9】

図 9 は本願情報処理装置の第 2 の実施の形態の別な例を示す基本構成図である。

【図 10】

図 10 は本願情報処理装置の第 3 の実施の形態を示す基本構成図である。

【図 11】

図 11 は本願情報処理装置の第 4 の実施の形態を示す基本構成図である。

【図 12】

図 12 は本願情報処理装置の第 5 の実施の形態を示す基本構成図である。

【図 1 3】

図 1 3 は本願情報処理装置の第 6 の実施の形態を示す基本構成図である。

【図 1 4】

図 1 4 は本願情報処理装置の第 7 の実施の形態を示す基本構成図である。

【図 1 5】

図 1 5 は本願情報処理装置の第 8 の実施の形態を示す基本構成図である。

【図 1 6】

図 1 6 は本願情報処理装置の第 9 の実施の形態を示す基本構成図である。

【図 1 7】

図 1 7 は本願情報処理装置の第 1 0 の実施の形態を示す基本構成図である。

【図 1 8】

図 1 8 は本願情報処理装置の第 1 1 の実施の形態を示す基本構成図である。

【図 1 9】

図 1 9 は本願情報処理装置の第 1 2 の実施の形態を示す基本構成図である。

【図 2 0】

図 2 0 は暗号化判定回路の一例を示す図である。

【図 2 1】

図 2 1 は本願情報処理装置の第 1 3 の実施の形態を示す基本構成図である。

【図 2 2】

図 2 2 は本願情報処理装置の第 1 4 の実施の形態を示す基本構成図である。

【図 2 3】

図 2 3 は本願情報処理装置の第 1 5 の実施の形態を示す基本構成図である。

【図 2 4】

図 2 4 は本願情報処理装置の第 1 6 の実施の形態を示す基本構成図である。

【図 2 5】

図 2 5 は本願情報処理装置の第 1 7 の実施の形態を示す基本構成図である。

【図 2 6】

図 2 6 は本願情報処理装置の第 1 8 の実施の形態を示す基本構成図である。

【図 2 7】

図 2 7 は本願情報処理装置の第 1 9 の実施の形態を示す基本構成図である。

【図 2 8】

図 2 8 は本願情報処理装置の第 2 0 の実施の形態を示す基本構成図である。

【図 2 9】

図 2 9 は本願情報処理装置の第 2 1 の実施の形態を示す基本構成図である。

【図 3 0】

図 3 0 は本願情報処理装置の第 2 2 の実施の形態を示す基本構成図である。

【図 3 1】

図 3 1 は本願情報処理装置の第 2 3 の実施の形態を示す基本構成図である。

【図 3 2】

図 3 2 はメモリセルアレーのひとつの例を示す図である。

【図 3 3】

図 3 3 は本願情報処理装置の第 2 4 の実施の形態を示す基本構成図である。

【図 3 4】

図 3 4 は本願情報処理装置の第 2 5 の実施の形態を示す基本構成図である。

【図 3 5】

図 3 5 は本願情報処理装置の第 2 6 の実施の形態を示す基本構成図である。

【図 3 6】

図 3 6 は本願情報処理装置の第 2 7 の実施の形態を示す基本構成図である。

【図 3 7】

図 3 7 は本願情報処理装置の第 2 8 の実施の形態を示す基本構成図である。

【図 3 8】

図 3 8 は本願情報処理装置の第 2 9 の実施の形態を示す基本構成図である。

【図 3 9】

図 3 9 は本願情報処理装置の第 3 0 の実施の形態を示す基本構成図である。

【図 4 0】

図 4 0 は鍵バッファの実装例を示す図である。

【記号の説明】

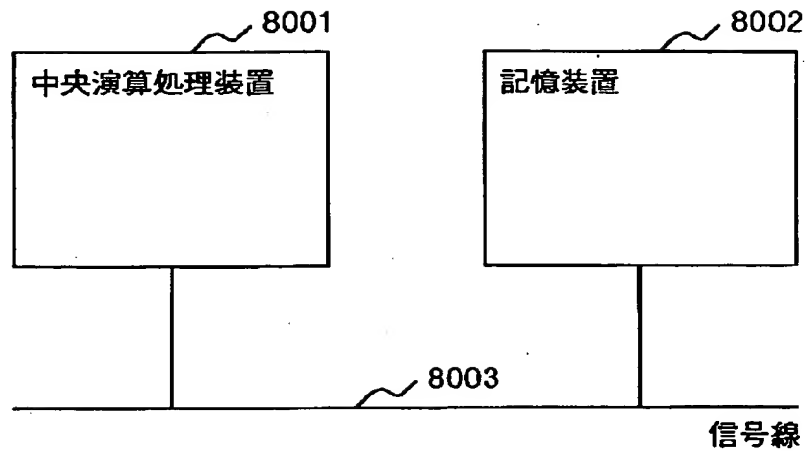
8001は中央演算処理装置、8002は記憶装置、51は半導体チップ、52はカード部材、53はリーダライタ、54はコントロールプロセッサ、55は磁気ディスク、0101、0401、0501は情報処理装置（ROM）、0102、0201、0251、0301、0402、0502は情報処理装置（CPU）、0202、0252、0302は情報処理装置（RAM）、1101、1301、1401、1501、1601、1701、1301、1401、1601、1701はデータ処理装置（CPU）、1102、1302、1402、1502、1602、1702、1302、1402、1602、1702はデータ処理装置（RAM）、0113、0213、0263、0312、0408、0506は信号線、0114、0115、0116、0117、0118、0119は電力発生装置、0309、0507はダミー信号線、0407、0505、5008はプリチャージ信号制御装置、5003は反転装置、51101はデータ処理装置、51102は情報記憶装置、51107、7007はデータバス、51108、7008はアドレスバス、7002はメモリセルアレイである。



【書類名】 図面

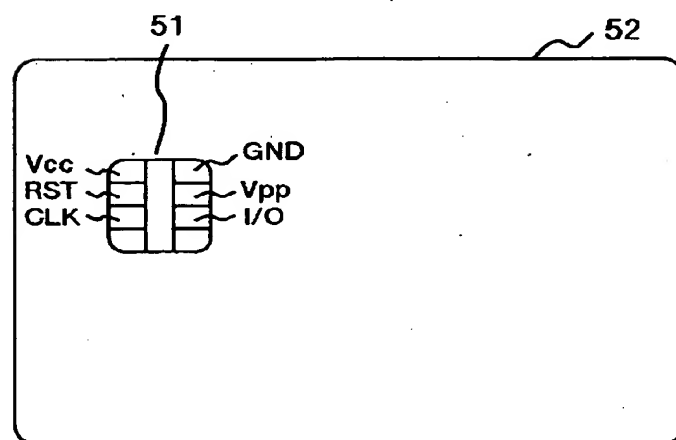
【図 1】

図 1



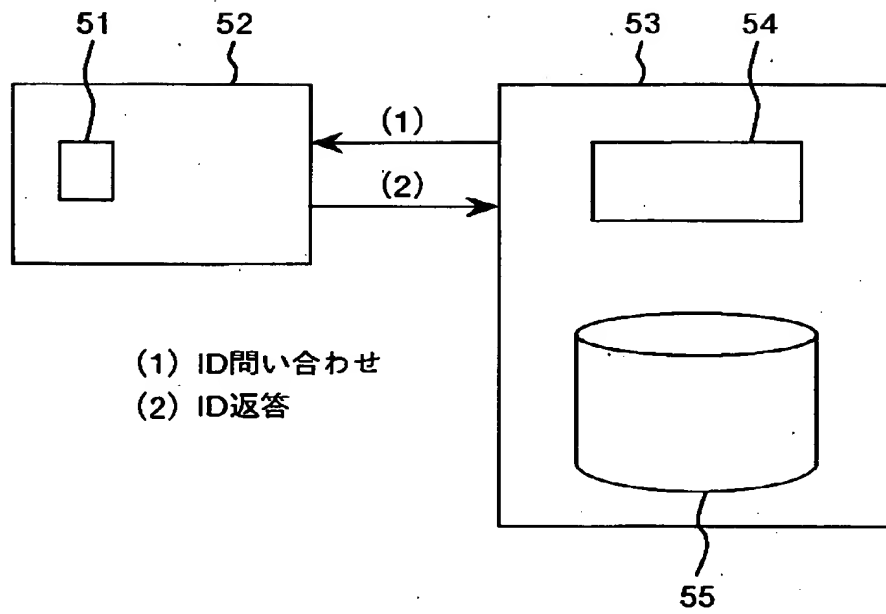
【図 2】

図 2



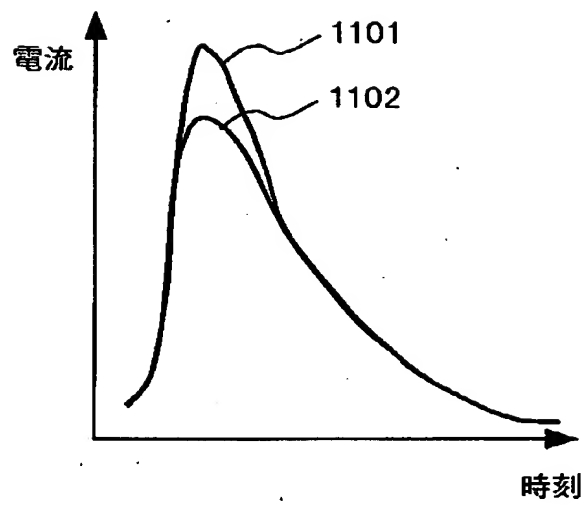
【図 3】

図 3



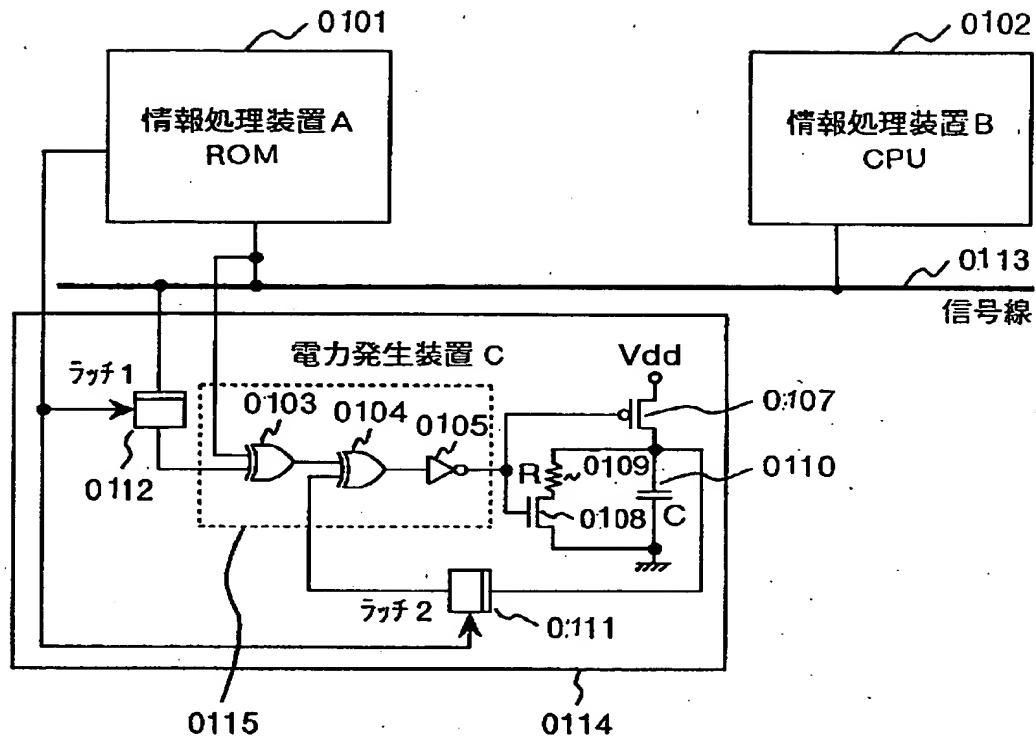
【図 4】

図 4



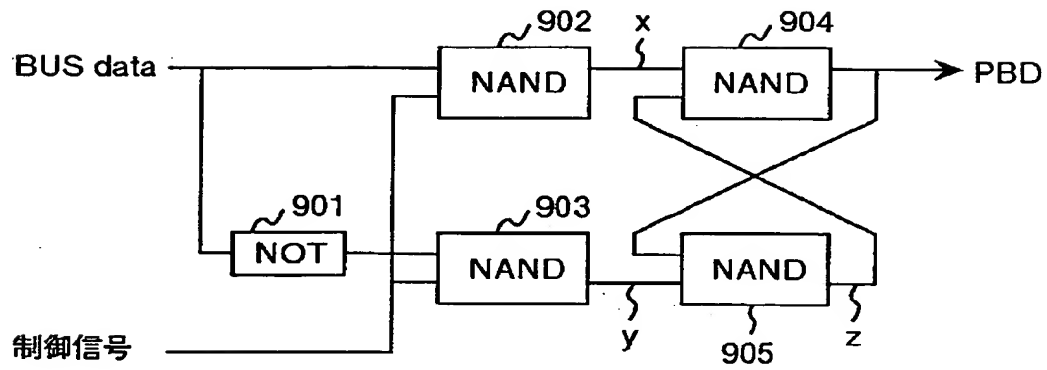
【図 5】

図 5



【図 6】

図 6



【図 7】

図 7

(a)

信号線の状態

1 1 0 0 1 0 1 0 0 0 1 0 0 1 0 0

コンデンサの状態

0 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1

(b)

信号線の状態

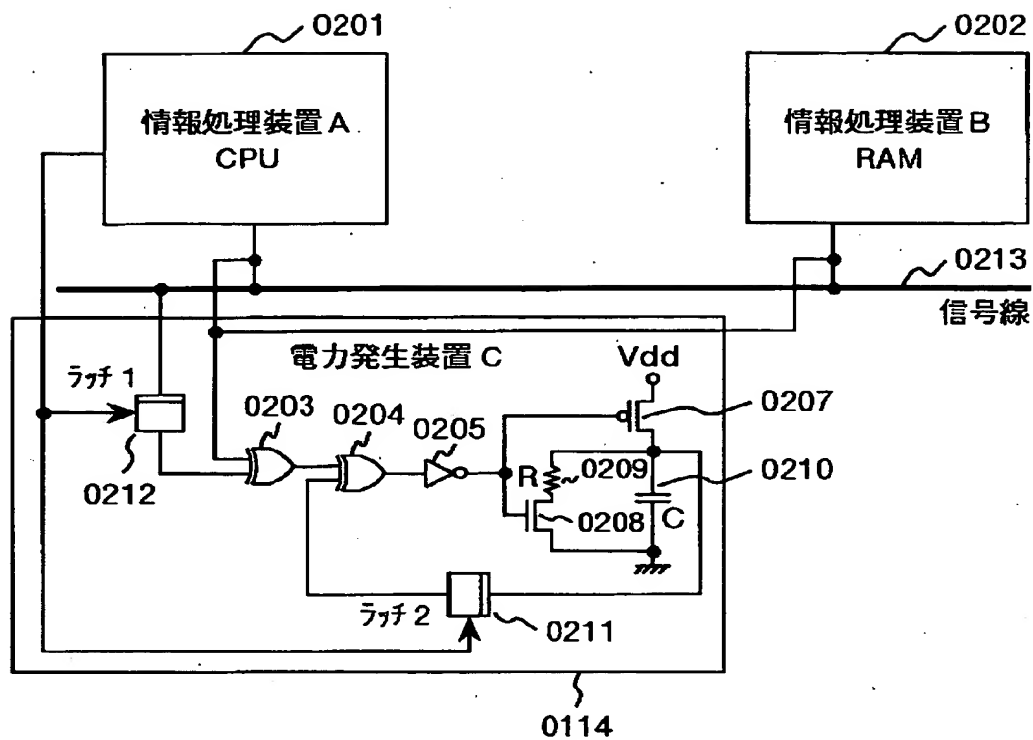
0 1 1 0 1 0 1 0 0 1 0 0 1 0 0

コンデンサの状態

1 1 0 0 0 0 0 0 1 1 1 0 0 0 1

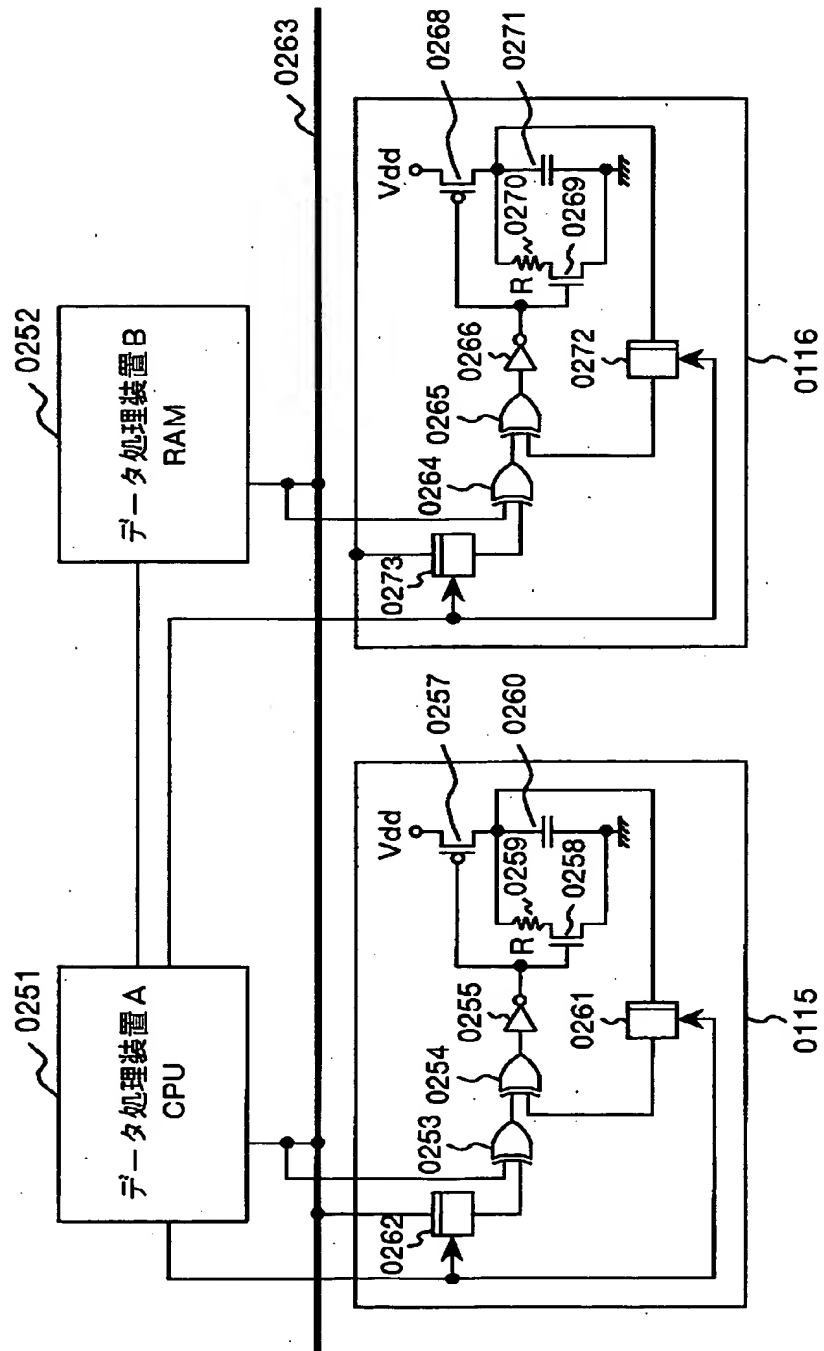
【図 8】

図 8



【図 9】

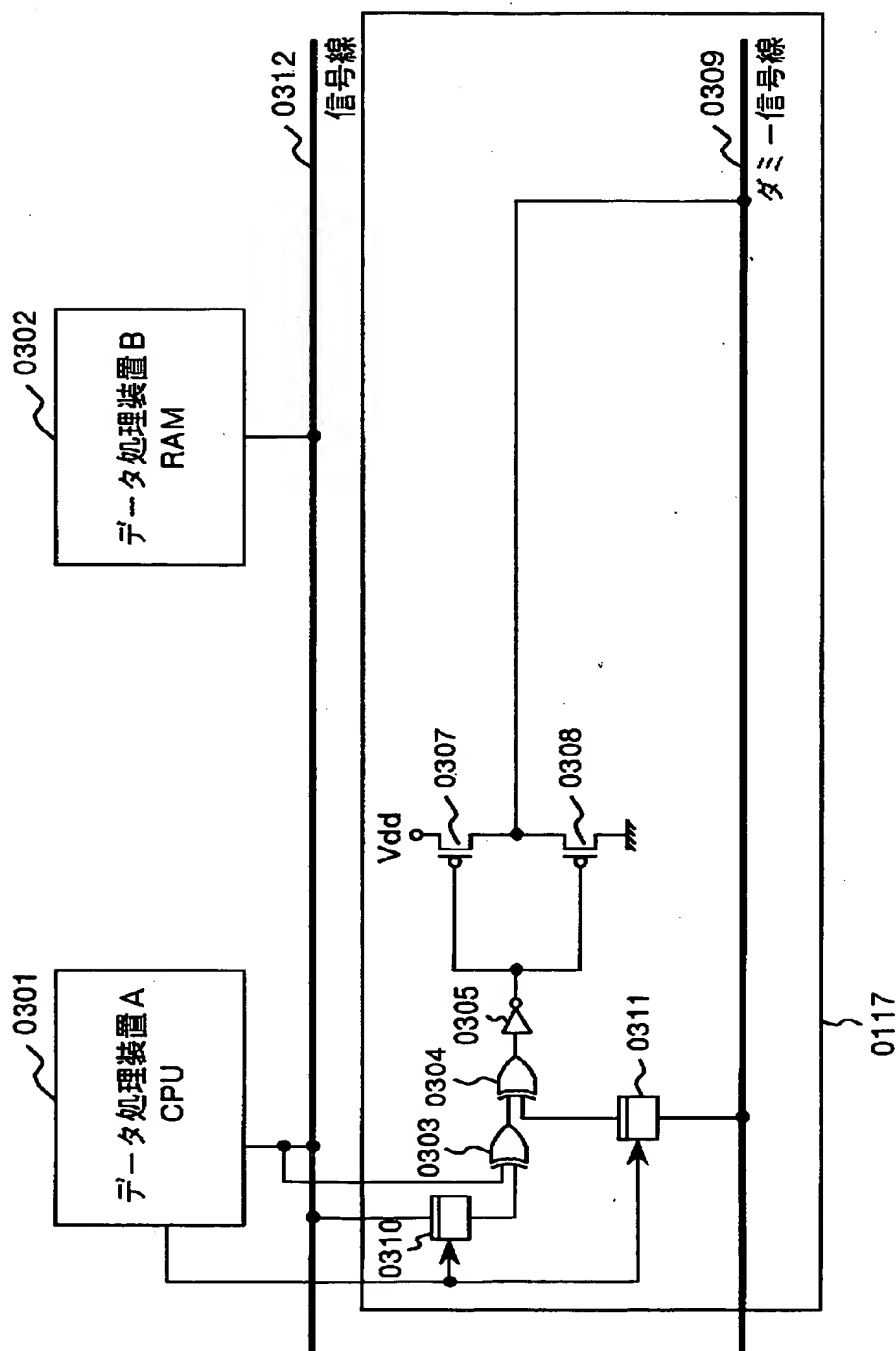
図 9





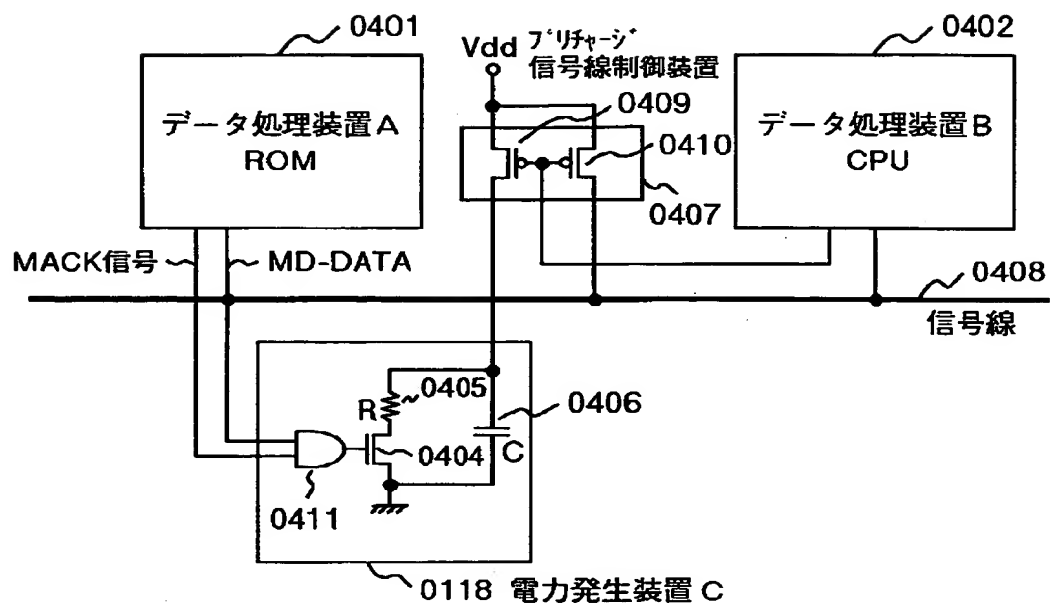
【図 1 0】

図 1 0



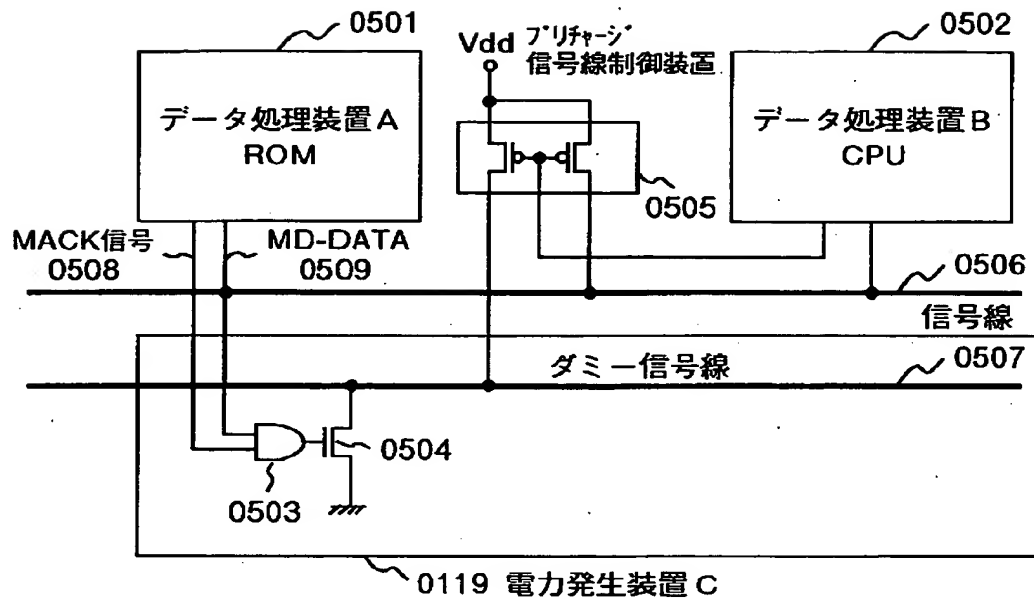
【図 11】

図 11



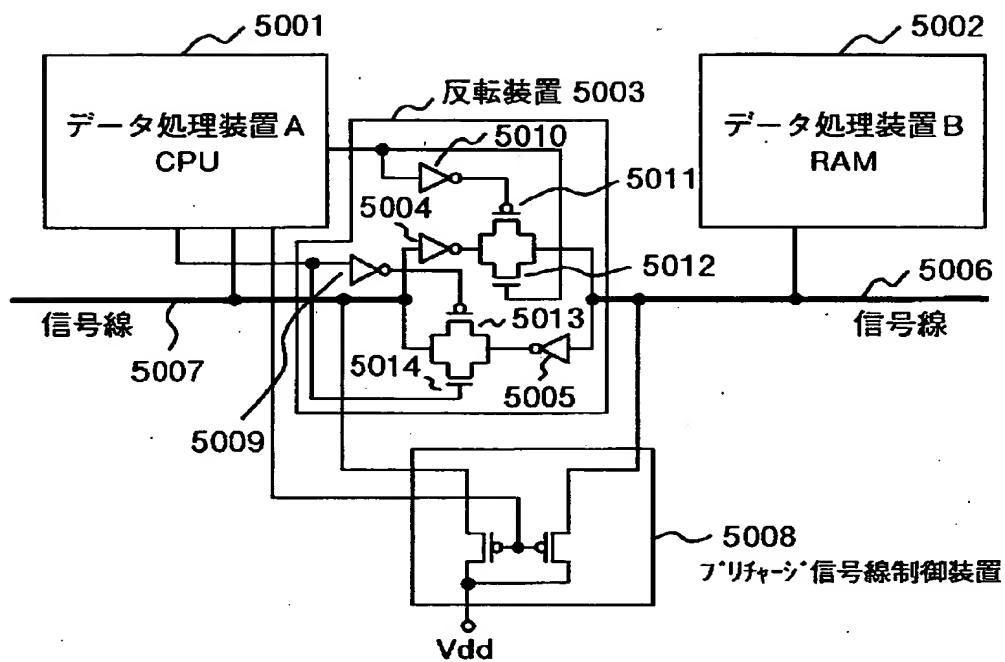
【図 12】

図 12



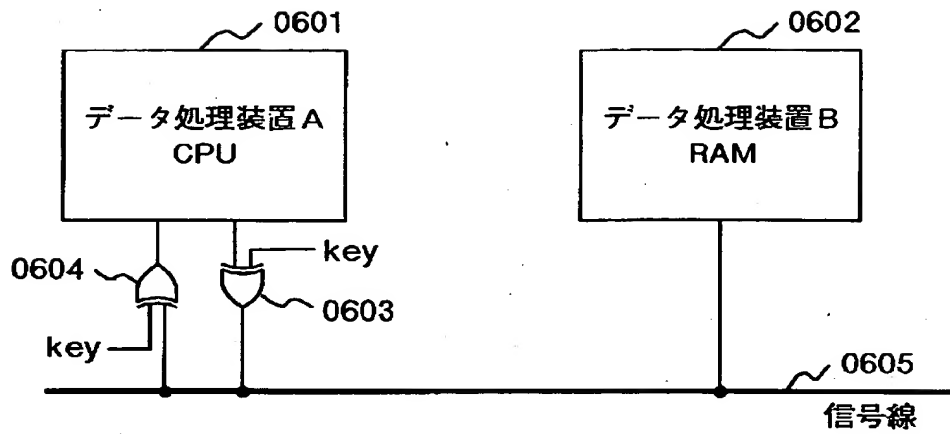
【図 13】

図 13



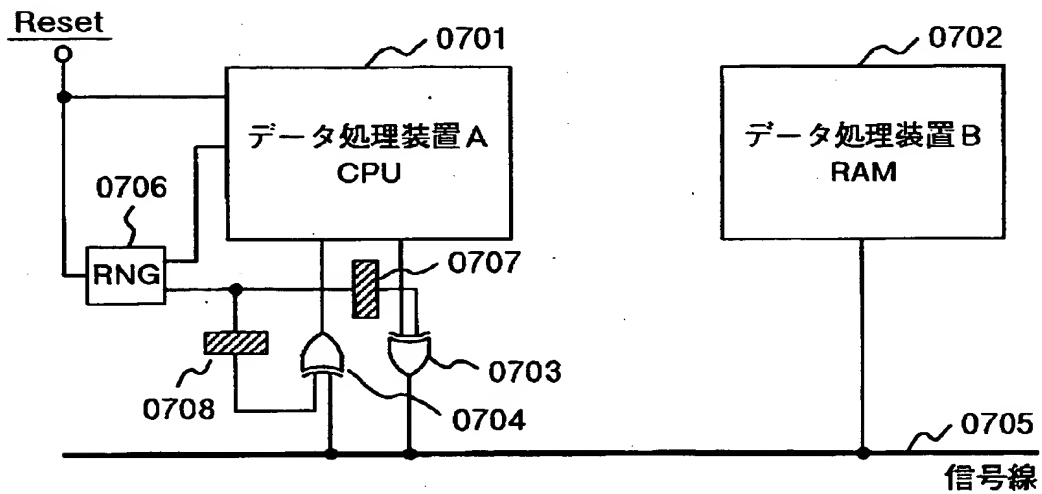
【図 14】

図 14



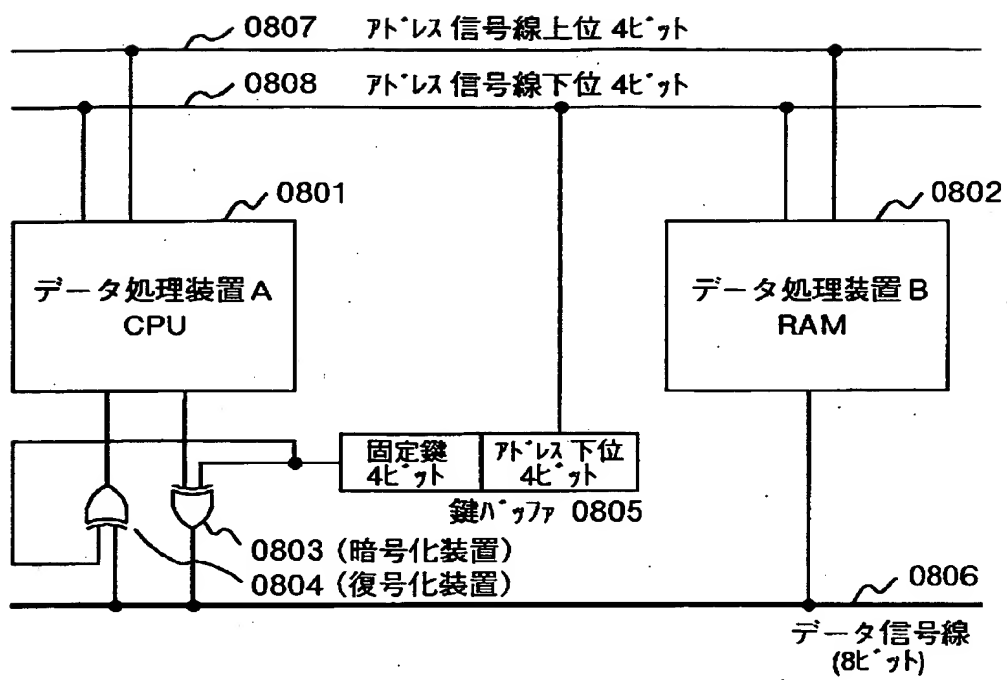
【図 15】

図 15



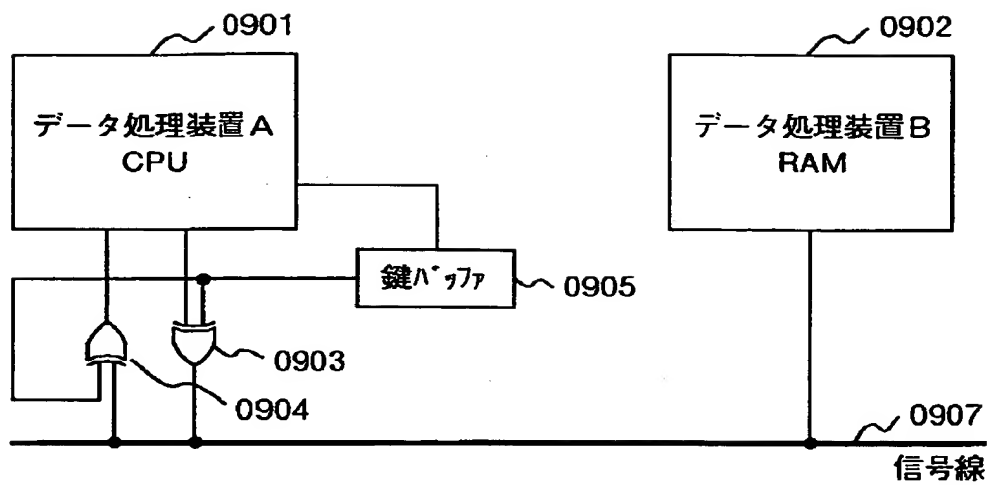
【図 16】

図 16



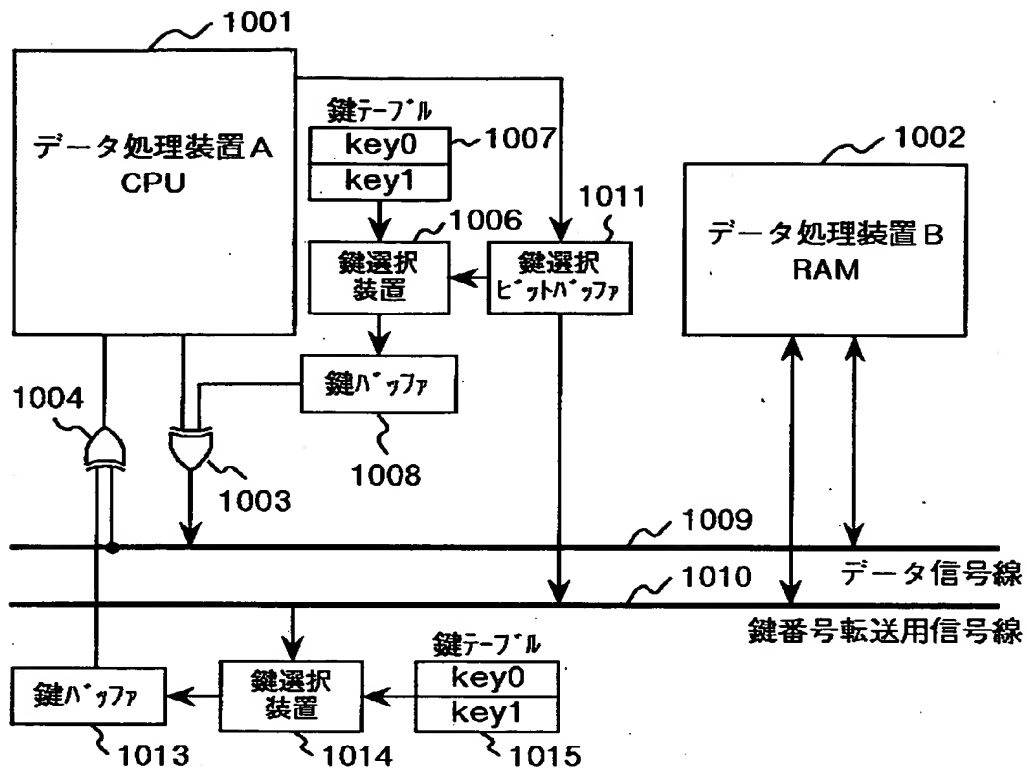
【図 1 7】

図 1 7



【図 1 8】

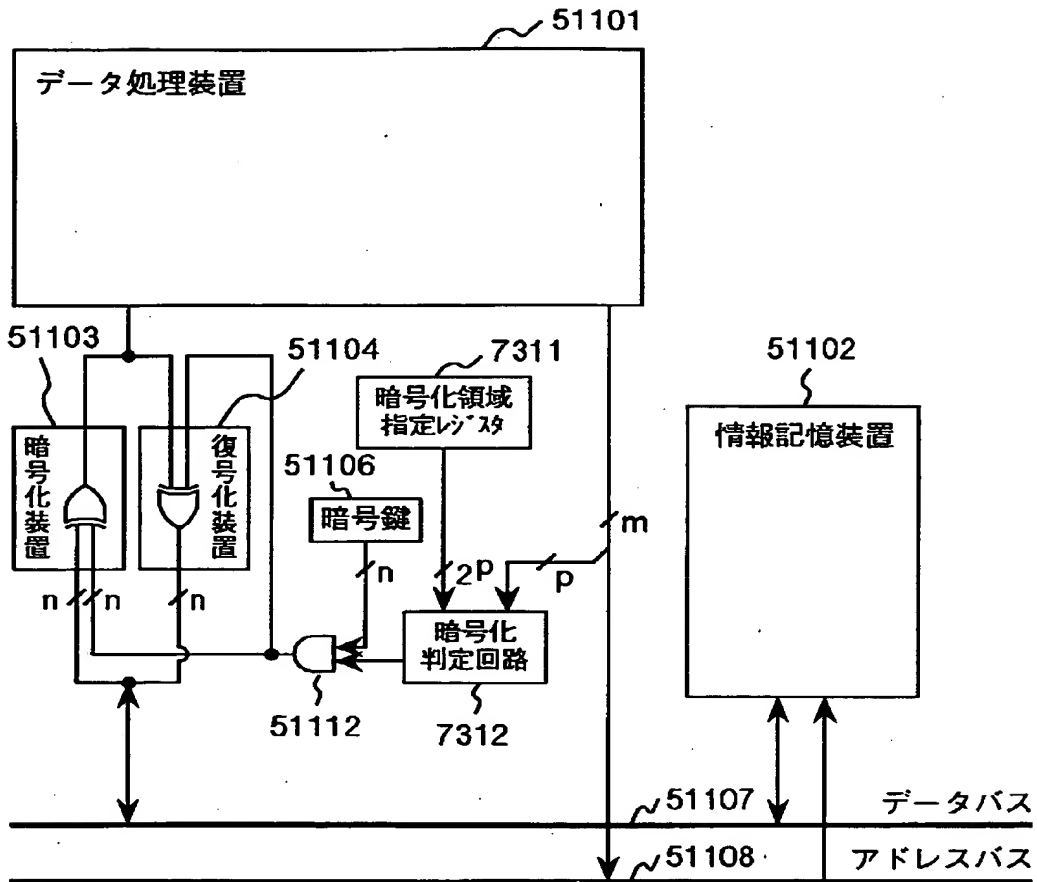
図 1 8





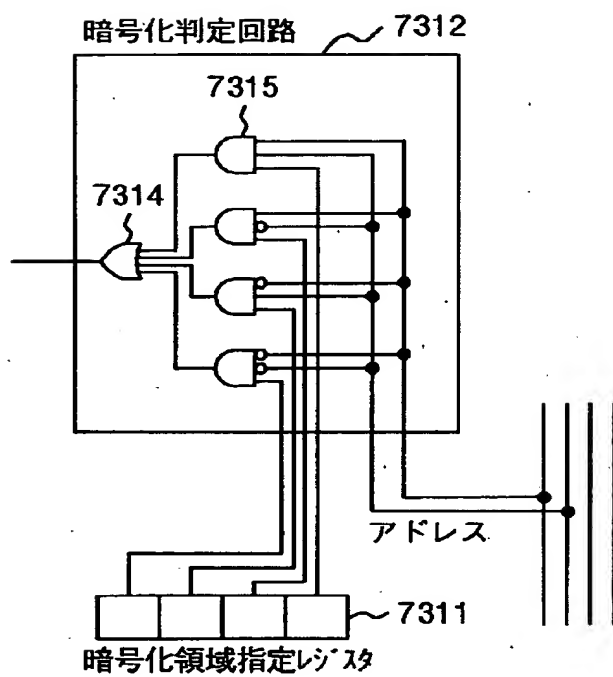
【図 1 9】

図 1 9



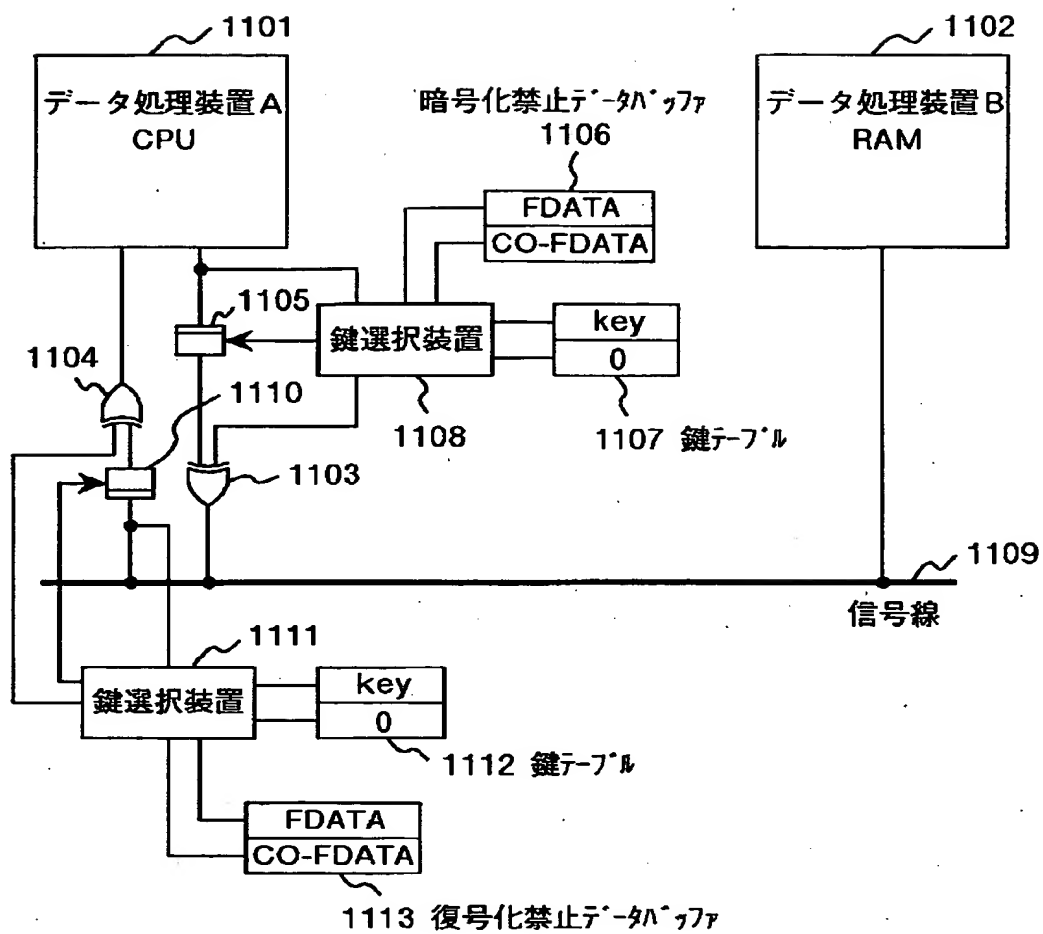
【図 20】

図 20



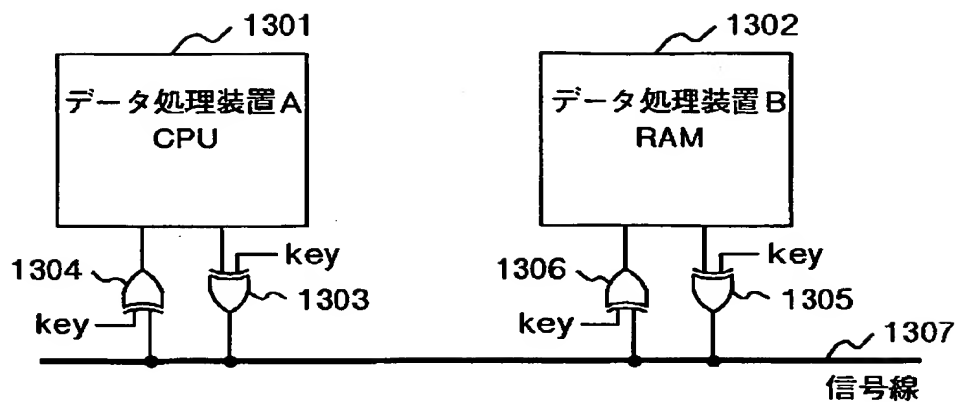
【図 21】

図 21



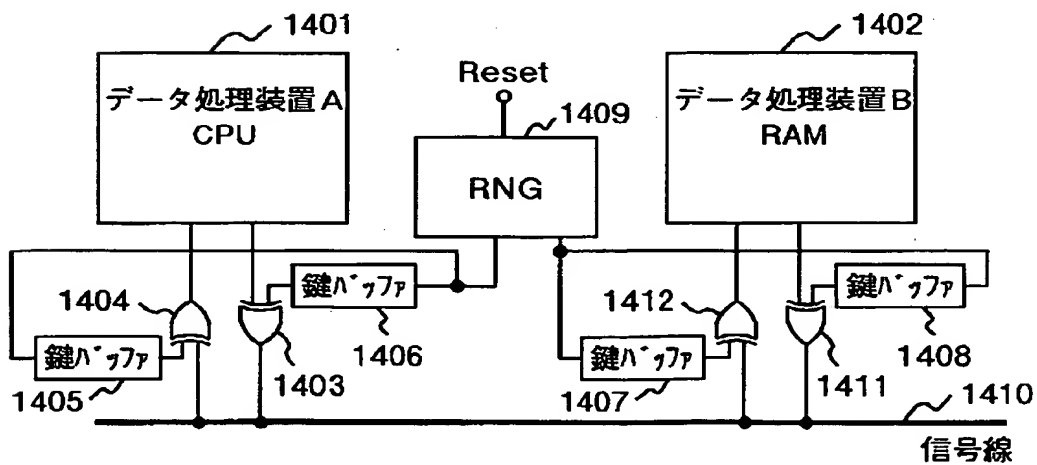
【図 2 2】

図 2 2



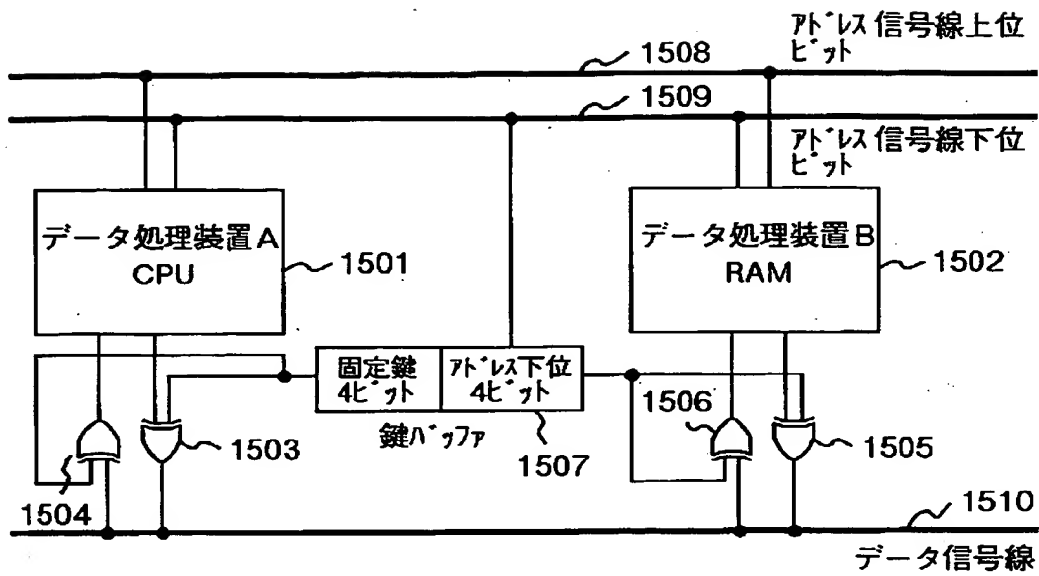
【図 2 3】

図 2 3



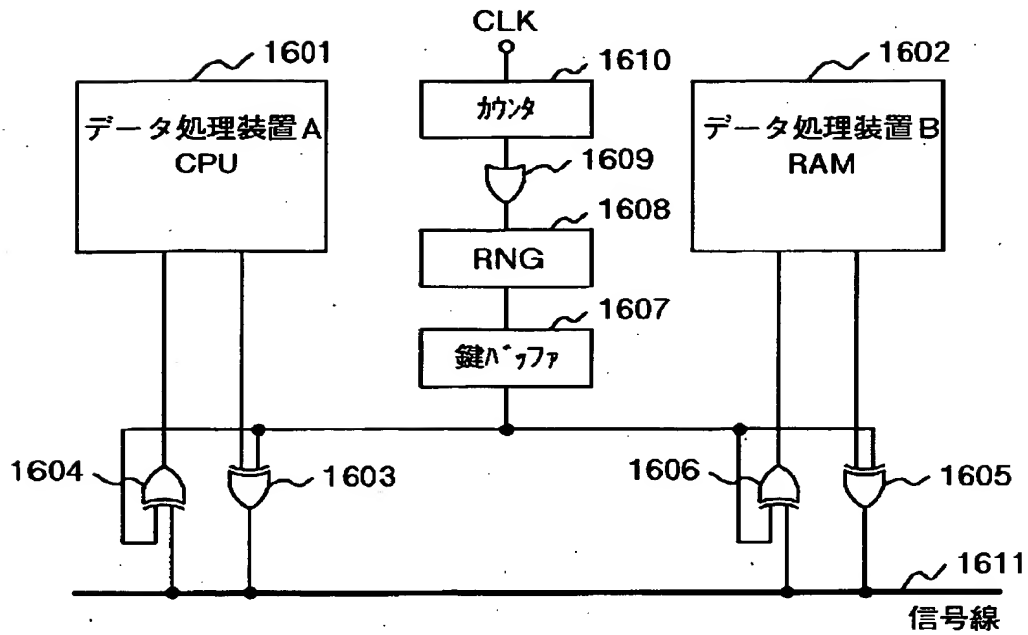
【図 2 4】

図 2 4



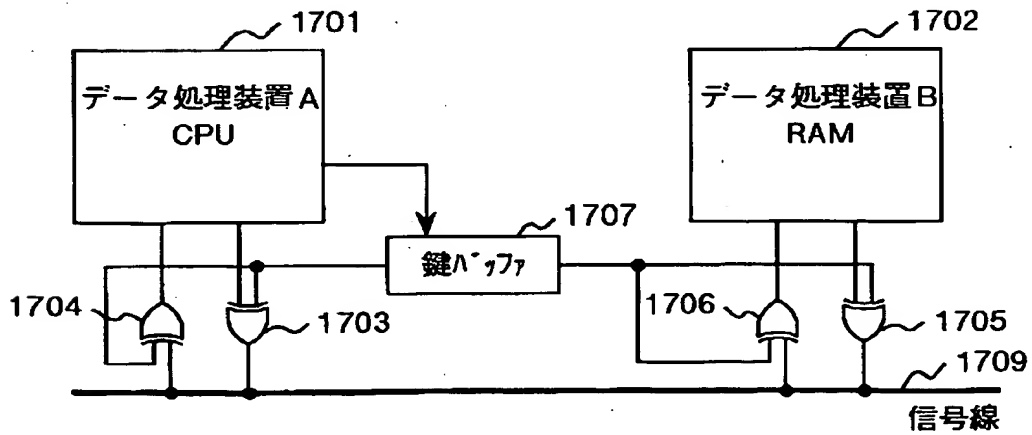
【図 25】

図 25



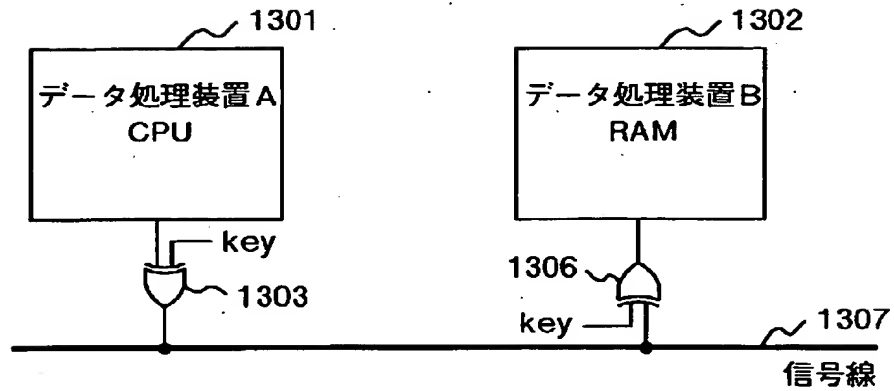
【図 26】

図 26



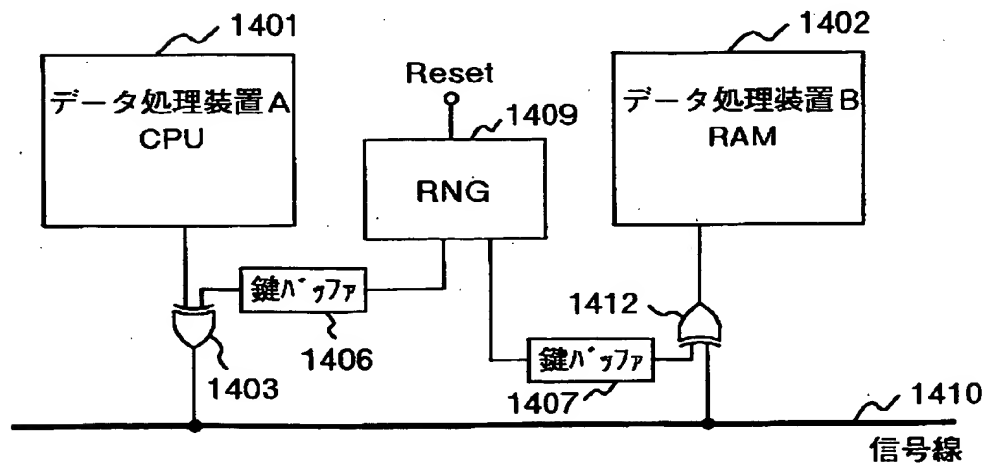
【図 27】

図 27



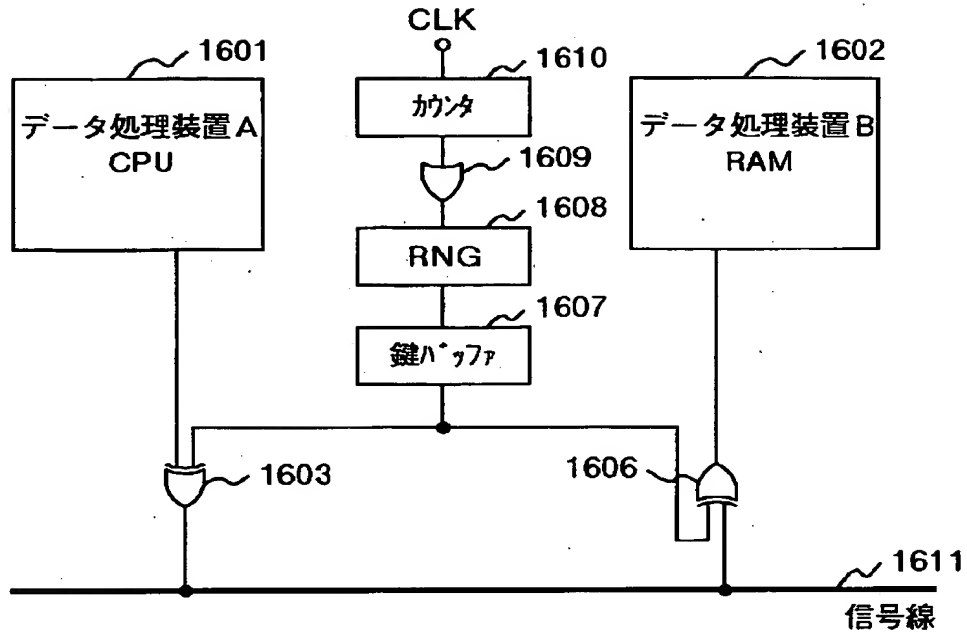
【図 28】

図 28



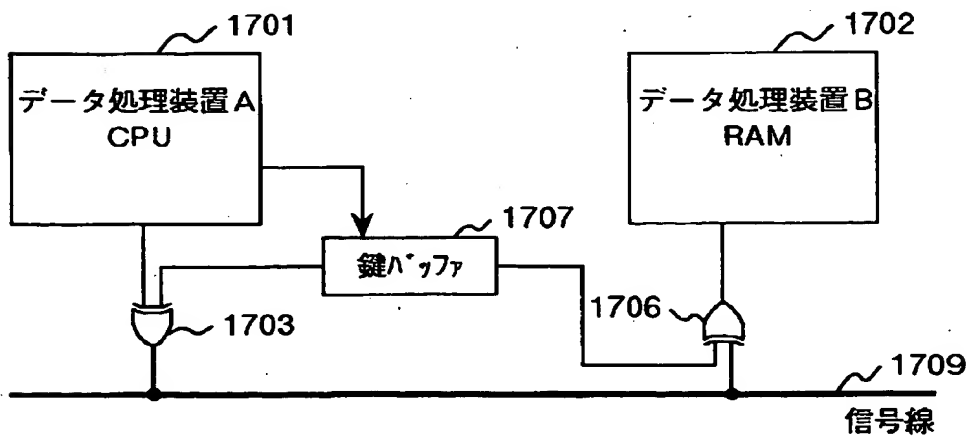
【図 29】

図 29



【図 30】

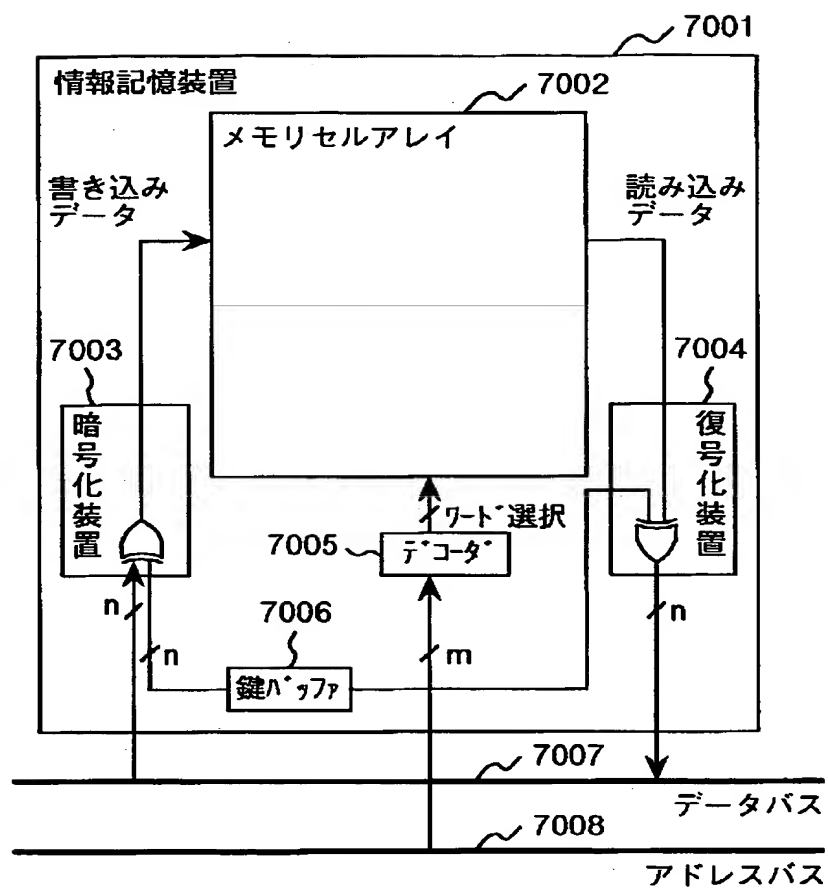
図 30





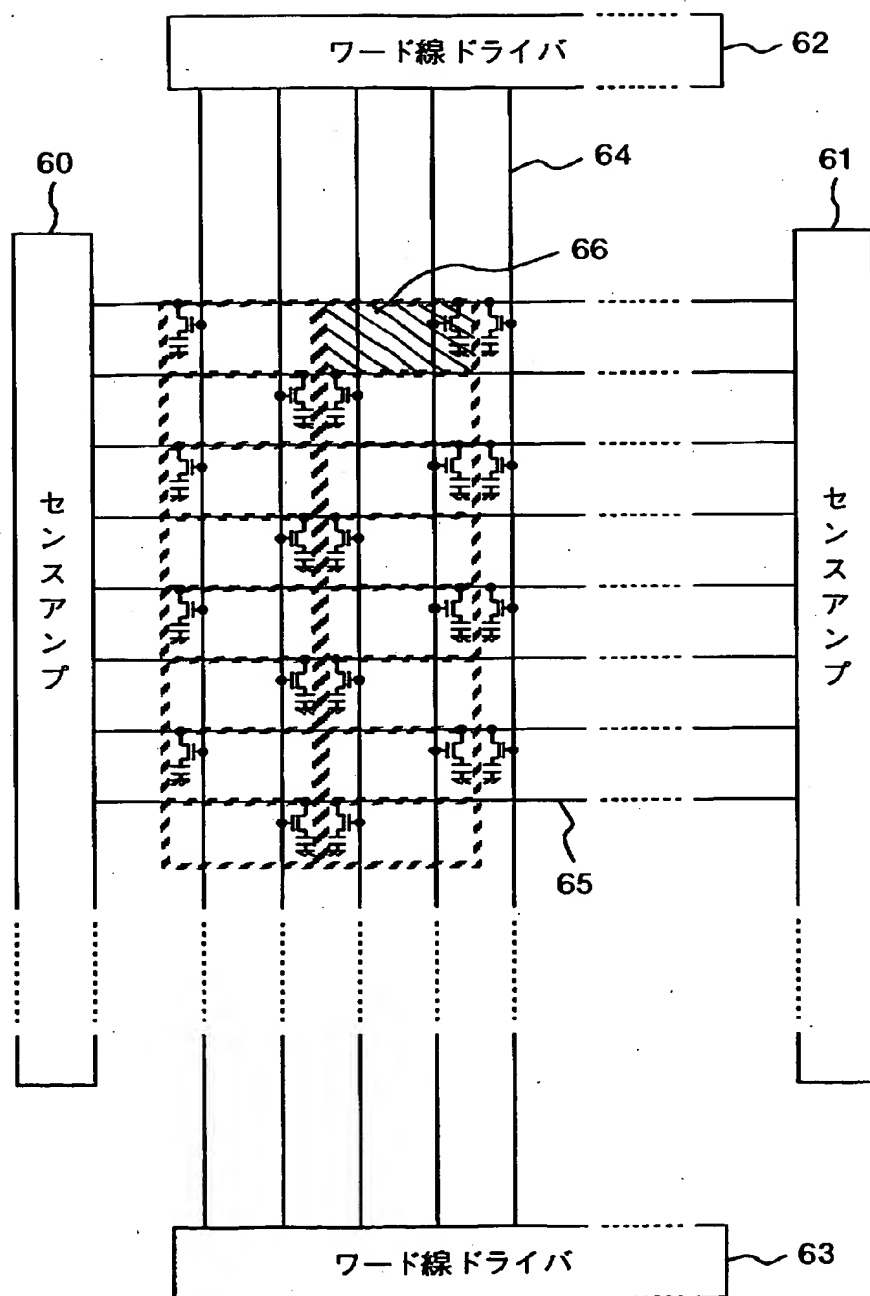
【図 31】

図 31



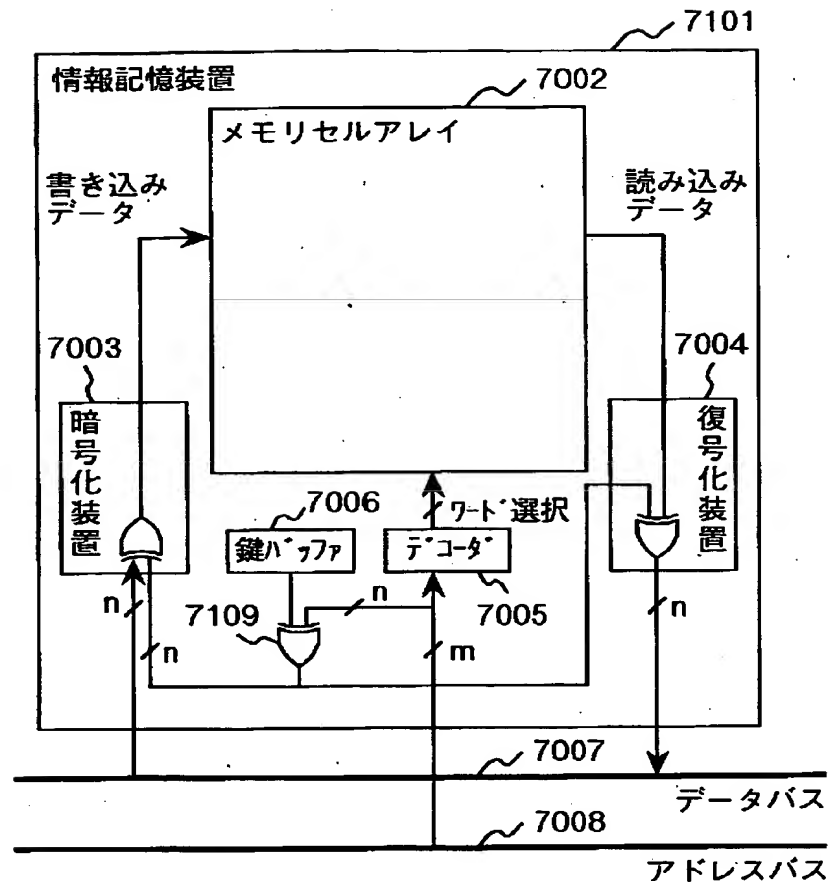
【図 32】

図 32



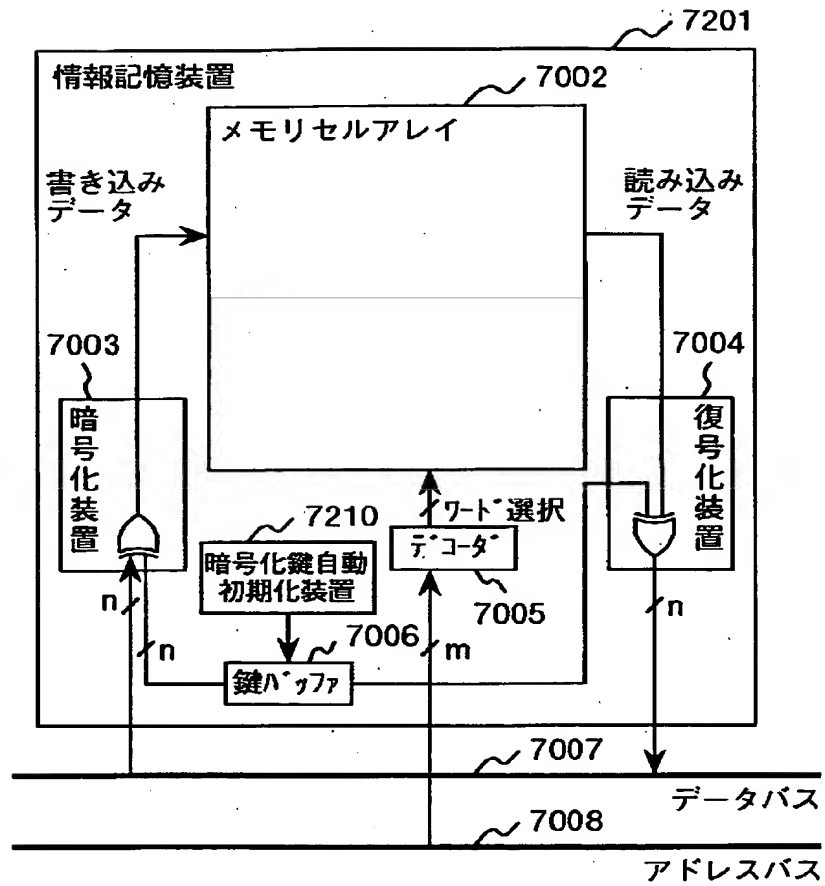
【図 33】

図 33



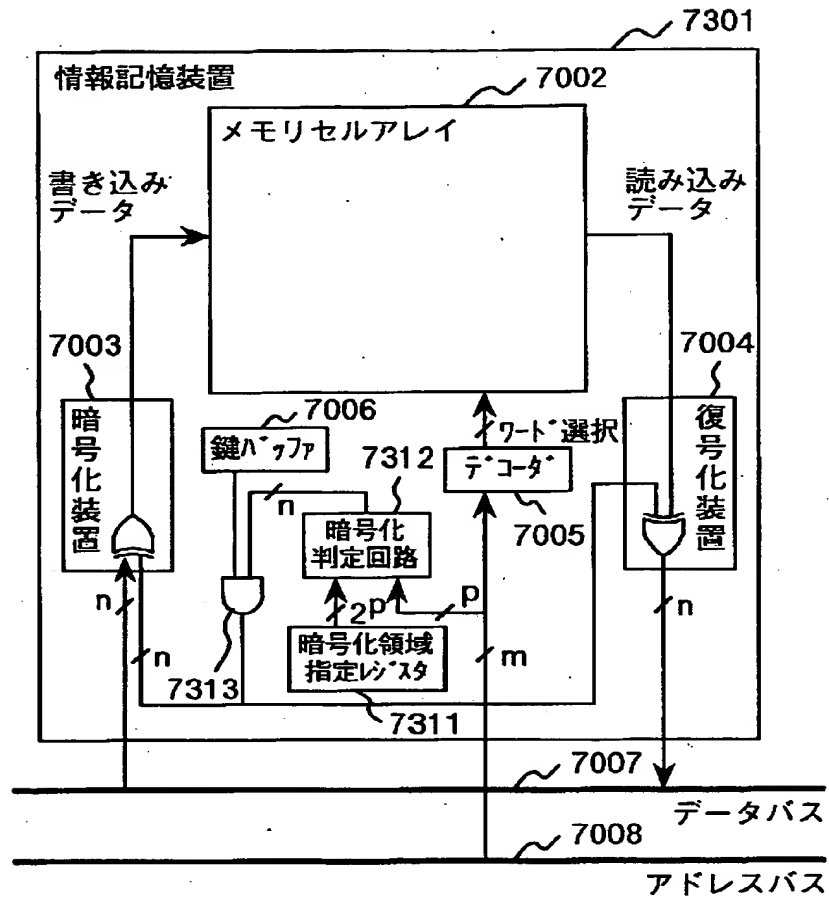
【図 34】

図 34



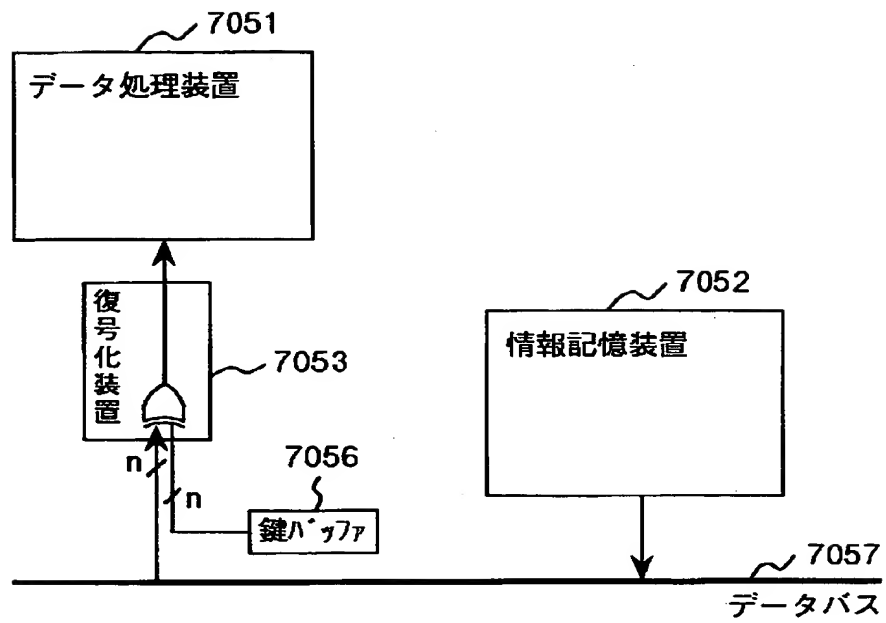
【図 35】

図 35



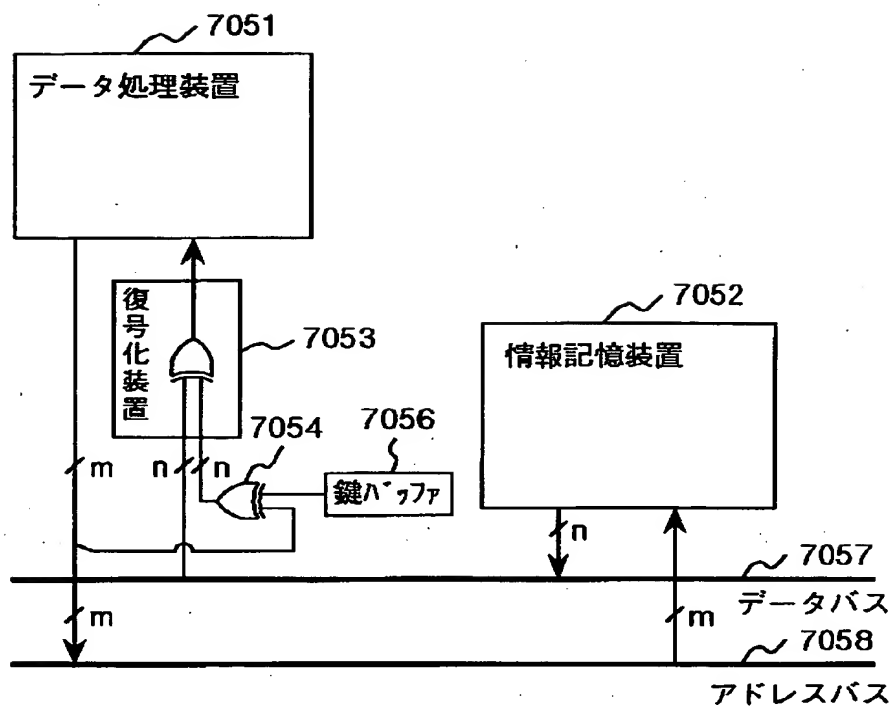
【図 36】

図 36



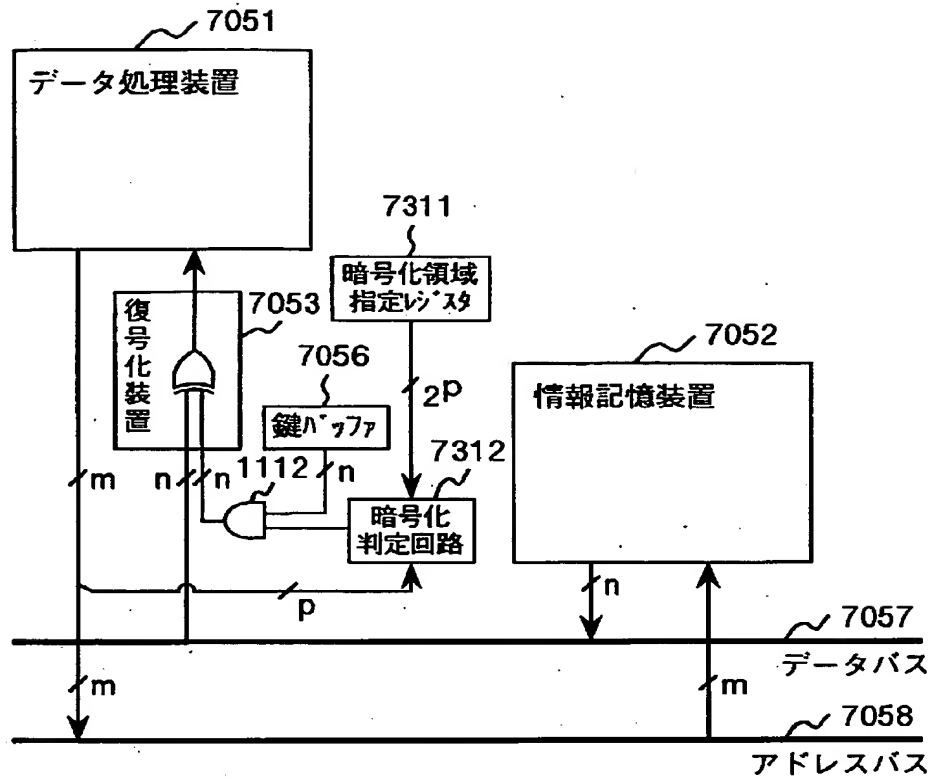
【図 3 7】

図 3 7



【図 38】

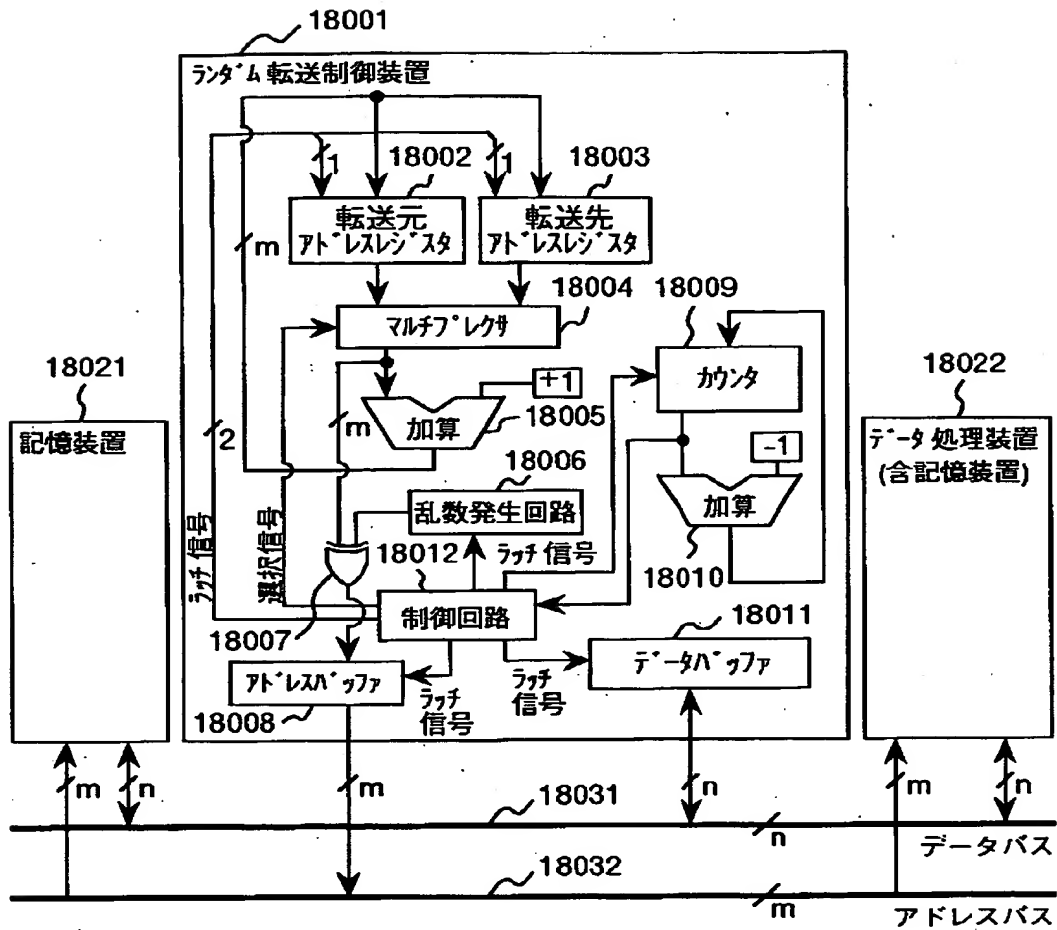
図 38





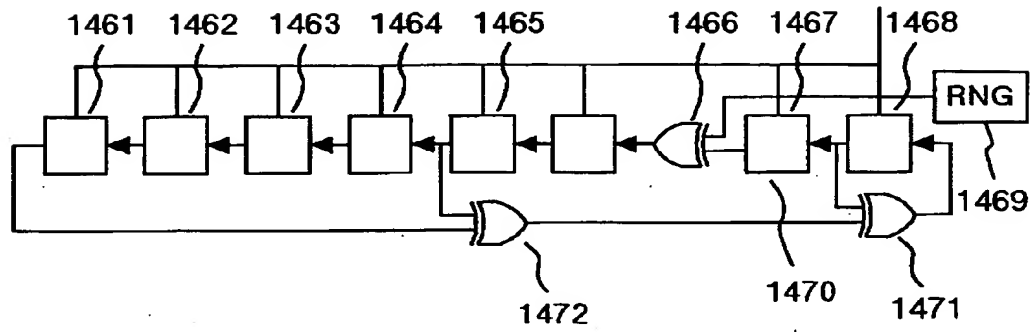
【図 39】

図 39



【図 4 0】

図 4 0



【書類名】要約書

【要約】

【課題】 本願発明は、高いセキュリティを持つ情報処理装置を提供せんとするものである。更には、本願発明は、高いセキュリティを持つカード部材、およびカード・システムを提供するものである。

【解決手段】 本願発明の形態は、情報処理装置と、当該第1の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされている情報処理装置である。本願発明の別な形態は、情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能な情報処理装置である。更に、本願の別な形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能な情報処理装置である。

【選択図】 図5

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [000233169]

1. 変更年月日 1998年 4月 3日

[変更理由] 名称変更

住 所 東京都小平市上水本町5丁目22番1号

氏 名 株式会社日立超エル・エス・アイ・システムズ